EUROSMART

The Voice of the Smart Security Industry

White Paper
Smart Security Market Segmentation

April 2008

Disclaimer

Eurosmart takes reasonable measures to ensure the quality of the information contained in this document. However, Eurosmart will not assume any legal liability or responsibility for the accuracy, reliability or completeness of any information contained therein and any consequences of any use.

Index

A preface from Eurosmart Chairman Jacques Seneca

It is often said that in life 'you get what you pay for'. Nowhere is that as true as in the field of security. Yet Eurosmart members are increasingly finding that, with respect to security, it is very hard for their customers to define what they need and to understand what they are paying for. There is a vast difference between the security that comes with commodity level disposable cards and tags and that provided by high-end Smart Security objects. Yet so often customers demand either too much security or too little.

Like quality, security is one of those features that it is hard to appreciate until you no longer have it. However, compared to the cost of completely recalling your card base or repairing a system wide breach, paying for the correct level of security from the outset is a wise investment. Upfront savings made from purchasing low cost, low security products when what you need is a high security solution can be very false savings indeed. Just think about the cost of repairing a breakdown in user confidence.

But equally, why pay too much for something you don't need? Just as you make appropriate purchasing decisions when you are investing in a car, or furniture or home electronics, with security you will do best when you buy what is fit for your purpose, be it low risk and low security or high risk and high security. This is true for both contact and contactless cards and in all application areas.

The problem is though that it can be hard for customers who aren't experts in the field of Smart Security to know what they want.

Eurosmart decided therefore that it would benefit everyone, customers and suppliers alike, to help educate customers about different levels of risk and how to choose the appropriate level of security for their system or application. We aren't aiming to duplicate existing security certification schemes. Those are technical schemes, designed to prove that products meet their security claims. Instead, we want to help customers understand the level of security they need to pay for.

This White paper is a major step in that process. We look forward to your feedback.

Jacques Seneca
Chairman, Eurosmart
24th April 2008

Part 1 – Introduction

As Jacques Seneca points out, the correct level of security to choose for an application is the appropriate level of security needed, no more and certainly no less. The purpose of this White paper is to help customers of the Smart Security industry to make the right purchasing choices based on an understanding of the risks they face. Fraudsters and criminals have many different ways of attacking card based systems, using hardware and software based attacks but this need not be a problem – the security to meet these attacks is available. It's simply a question of making the correct purchasing choices.

The paper will explain the main types of security risks arising from those attacks and how they apply to the major application areas for Smart Security technologies. It will explain the need to link those risks to corresponding security requirements and thus the correct level of Smart Security. It will then present a methodology for assessing risk and purchasing the correct level of Smart Secure technology.

1.1 Executive summary

In all application areas for Smart Security objects, fraudsters and criminals are actively seeking ways of attacking systems. Because Smart Security objects are so widely used in daily life, those attacks can have multiple disastrous effects, both for end users and for system operators.

However many such attacks succeed because the incorrect level of security has been chosen for the system, due to a lack of full understanding of the risks involved and the product security implications of those risks.

Highly secure Smart Security technology is easily available from reputable vendors. Choosing it is simply a matter of better understanding specific application risks and their impact. This can be done by assessing at a number of factors including the cost and ease of committing an attack and its likely impact in terms of financial and other losses, inconvenience and probability. This assessment can then be used to correctly specify and purchase security for a Smart Security technology system. In that way, the system operator can be sure that they have neither under- nor over-purchased security.

Part 2 – Understanding the risks

Smart Security objects (in general smart cards) are a major part of our daily lives. We use them for banking, for telecommunications, for travel, in the healthcare sector, in the workplace and increasingly for public sector applications like identity, driving licences and passports. As SIM cards hidden inside our phones they protect and enable our access to GSM networks. In our wallets, they allow us to make payments in the physical world with far greater security than magnetic stripe cards do. They store or protect access to our medical data. They store biometric identification data, proving our identity. In their contactless variant they speed us through transit barriers and low value payments.

Some of these uses come with a need for high security, others less so. Some already are well protected, others might benefit from changing the level of security they offer, either up or in some cases, where the system has been over specified, down. Risks can be gauged from a number of factors, including the technologies used in the system, the assets that require protection and the people who use the system. Protection levels can be assessed from the Smart Security already used and from how regularly it is replaced – technology and with it risks continually change and mutate and it is vital to use the latest technology to combat the latest threats.

This part of the paper will examine why security is so important, will describe some common attacks and will look at specific use cases in more detail.

2.1 The need for security

Because system users and owners have assets to protect, be they personal identity, money, privacy, intellectual property, state security or others, it is important for systems to have security. The more valuable the assets are, the more likely a system is to be attacked. Using Smart Security objects as protection can provide the appropriate level of security for a wide range of different risks.

However it is important to choose the correct level of security. Security has a cost so it is worthwhile using a risk management approach, which balances the cost of security against the potential losses. The first step in risk analysis is to identify the asset to be protected. The second step is to analyse the vulnerabilities and the possible attack scenarios that threaten these assets. Finally estimate the risk, and identify the best compromises with countermeasures to be implemented within the system and/or the security device.

This document will look at different use cases for Smart Secure Devices, classified according to application area for the device. Each use case will look at the assets that are at risk, the threats, risk factors including probability of occurrence, the impact of occurrence, including where appropriate damage to reputation and credibility and the ideal replacement cycle for cards in that application. It will also examine means of protection and the level of security needed to counter the threats.

Clearly, the motivation of the attackers will depend on the level of assets that is at risk. In addition the probability of an attack is not the same as the probability of a successful attack.

We will be assigning security levels of basic, medium and high to different use cases. Each level will cover a range and there may be some overlap between levels. For example basic security could range from no security at all to a moderate level of security.

In all cases, security should anticipate rather than follow attack scenarios. While attackers may use expensive high tech equipment for certain attacks, this is not always the case – they may simply be very clever. In addition, high tech equipment may be less available to hackers making economic attacks than to university researchers for example.

Because fraudsters and criminals are continually working on developing new attacks, security erodes over time. Therefore it is vital to understand the concept of the renewal cycle, where cards and smart objects are replaced with the latest smart technology on a regular basis to ensure that they use the most up to date technology and protections. Clearly, for the purposes of security, the lifetime of the product used or its renewal cycle starts with the introduction of the product onto the market and not with the date of its purchase by the user.

But first of all, it is worth examining briefly some of the attacks that fraudsters may use.

2.1.1 Types of attack

Attacks fall into four basic kinds – physical, side channel, faults and logical.

Physical attacks, using electron microscopes and laser beams can take months to develop and days to execute. One example is microprobing - this is done by opening the chip packaging, placing small metal needles on the lines of the chip and recording and analysing signals on the probed line. These lines will be easily visible on unprotected chips. Alternatively, the attacker may grind the chip down, layer by layer. Every layer will be photographed and the attacker can then reverse engineer the circuit and the stored contents of the chip. Memory content is easily visible on an unencrypted chip. Often physical attacks will simply destroy the chip but where they are successful, they will reveal secrets such as keys and authentication data held in the chip memory.

Side channel attacks listen in to the power consumption or emissions of the card and use statistical techniques to deduce what's happening. The attacker may be able to guess the keys from the observation of many cryptographic operations and statistical analysis. These attacks are non-invasive. Observation attacks, such as differential power analysis, can take days to develop and hours to execute. Analysing the power consumption of the chip allows the attacker to make deductions about the cryptographic keys used by the chip. It also provides information about the operational state of the chip.

Fault attacks techniques deal with external disturbance of code execution. By inducing errors in the operation of the chip, the attacker can gain information about the chip or circumvent software. Errors can be created with power spikes, electromagnetic radiation, light and alpha radiation.

Logical attacks attempt to crack cryptographic algorithms stored on the card, using sheer computing power and mathematical techniques. These can be both expensive and very time consuming to carry out. They are used to retrieve or modify information, without destroying the card.

Attackers are likely to use a combination of techniques – for example a non-invasive attack may follow an invasive attack, to gather further information. Once an attacker has refined an attack on a specific chip, he will be able to use it to quickly either copy smart card chips or reveal system secrets being held on the chip.

Card information can also be obtained by interfering with data transmission between the card and its host system. If the card is contactless, the wireless communication can be intercepted. Data from contact cards can be copied while the card is in a

reader device. In both cases, if the card data is not adequately protected, secrets may be revealed. Of course, it is also simple, quick and cheap to copy card data on the magnetic stripe of the card.

However the information is obtained, it can then be loaded onto blank cards and used fraudulently. Alternatively, the attacker may be able to remove protections on existing cards or alter the information on them.

2.1.2 Security levels

Whatever the level of security needed, the Smart Security industry can provide a suitable combination of hardware and software remedies to provide cost effective protection against attacks.

A **basic** level of security is associated with memory cards. These include some hardwired security logic and allow data modification or writing to the card only with the use of a password or PIN code. That means that the card can easily be read but only authorised people can change the data on the card. A typical use might be to store loyalty points. However if the card is used in an unsupervised terminal there is a risk that attackers could use cloned or emulator cards or could observe the password.

An additional security measure could include cryptographic authentication to prevent card copying. Secure memory cards with this feature are used as prepaid phone cards for public telephones – everyone can read and decrease the value stored on the card but security features prevent the unauthorised increase or reloading of value.

Many RFID or contactless chips fall into the category of basic security. Most allow value to be read but not freely modified. Some simply transmit a serial number. However it is very important to distinguish between basic RFID or contactless and what Eurosmart calls ‘Secure contactless devices’, such as those used in passports, which come with much more advanced levels of security.

A **medium** level of security is associated with systems where there are some assets to protect and a basic level of protection only would pose unacceptable risk. A typical example where the assets relate to one specific user would be corporate ID in a company without significant intellectual property to protect. The card owner himself might be a security risk if he is able to modify the system to grant himself higher access rights than he is entitled to. In this case, two-factor authentication is necessary to ensure that only an authorised administrator can amend access rights.

To determine the correct security measures to take, a risk analysis is needed. However typical measures taken at this medium level might include a strong algorithm with sufficient key length and a robust authentication protocol to avoid any disclosure of the keys. In addition it may be considered appropriate to include some countermeasures considered necessary at the high level of security, as defined below.

Smart Security object chips at this level of security might also feature active protection against attacks (such as sensors to detect operation out of normal operating range, an active shield to detect physical tampering), hardware services,

such as an embedded cryptographic engine, hardware encryption of memories and chip internal data handling and improved resistance against side channel attacks.

A **high or very high** level of security is associated with very sensitive systems where attacks are made against the entire system rather than against individual smart tokens and where the potential level of return is high. One example might be mobile television but the exact meaning of high security will differ from area to area. Other examples might be banking cards or government ID cards.

Countermeasures will therefore have to be able to guard against attacks by Smart Security experts using sophisticated and expensive equipment and which may take several years of experimentation to perfect. This level has been defined in the Common Criteria standard, which is used for certification, and quantified by the Smart Security community in “Application of attack potential to smart cards” (http://www.commoncriteriaportal.org/supdocs.html).

Typical countermeasures might include user authentication, administrator authentication, a robust exchange protocol over a secure channel, a strong algorithm and a key length that guarantees long term security. It is also highly recommended to use a smart object designed with a high attack potential in mind. This may have features including hardware sensors, encryption of stored data, integrity checks, random reading, and specific techniques for cryptographic calculation. In this case the concept of the renewal cycle for the smart objects is particularly important – in some cases, that cycle may need to be as short as one year.

Hardware measures, in addition to those listed above for basic and medium, will include state of the art active protection against all relevant attack methods, including reverse engineering, logical attacks, side channel, and fault injections which even the best prepared attackers will not be able to defeat. By definition this highest security level is constantly evolving. Hardware and software have to be perfectly adjusted with close co-operation between all industry actors to offer highest security together with performance at a bearable cost.

Two other factors are important to consider. In all of these areas, the user perception of the security level is just as important as the actual security level, however ill informed that perception might be. Furthermore, we also recommend mandating an external laboratory to perform an independent evaluation of the efficiency of the counter measures used.

2.2 Use cases

Now we will examine issues specific to different application areas for Smart Secure objects.

2.2.1 Corporate ID

Corporate ID cards are designed to protect corporate proprietary information. They are usually used for physical and logical access but the sensitive application is giving employee cardholders logical access to corporate IT systems.

Assets at risk are company confidential information, including corporate intellectual property, research data, strategic information, customer data, payments data and employee data.

The probability and the impact of these threats on company activities depend entirely on the industry sector and the company in question. They can vary from very low to quite dramatic. Company locations carrying out leading edge research in commercially sensitive areas will be at greater risk than those involved in more mundane activities. Each company will need to carry out a risk analysis to determine the types of risk it faces and the levels of protection it needs.

There are several ways an attacker could proceed – stealing a card, cloning a card or modifying access rights.

Stealing a card is simplest. If the card is not linked specifically to the cardholder, it will allow anyone access to company assets. This is in fact a basic level of security and may be appropriate if the impact of theft is judged to be low. A background system might provide some protection by allowing for the deactivation of the lost or stolen card.

Cloning a card allows the fraudster to impersonate an employee. It is more difficult for a background system to detect the fraud, but cloning also requires more expertise and mounting the attack will be more expensive. It is possible to protect against cloning by storing a certificate on the card (e.g. PKI), along with a robust algorithm. Then the card cannot be duplicated if the keys that are used for the generation of the authentication certificate cannot be retrieved. This protection is recommended when the risk is evaluated between medium and high. Another option is to issue the cardholder with a PIN or password.

Modification of access rights is likely to be an inside attack. It can be prevented by allowing only authorised administrators to alter card parameters. Where the risk is deemed to be higher, two-factor authentication may be necessary – a PIN code for the user and the storage of a certificate on the card.

Therefore security levels in this area may vary in general from medium to high. Given the speed of technical progress, we recommend a replacement cycle of around five years for cards used for this purpose, as this corresponds to significant improvements in technology and therefore an increase in vulnerability.

2.2.2 Passports

Electronic passports are used for identity checks and the assets involved are identity data, biometric data and government signature keys. Perception of threats may vary - users may be concerned about privacy of data – government authorities are more likely to be concerned about integrity of data.

The main threats to passports are counterfeiting, modification of data, denial of service and disclosure of data to non-authorised entities. The probability of occurrence of each of these threats is high, except for denial of service where the probability depends very much on where the border in question is located. The impact of each is high, except again for denial of service where the impact is low – passports will retain all their physical features and can be read in the traditional way if the electronics fail.

The International Civil Aviation Organization (ICAO) has provided specifications for Machine Readable Travel Documents (MRTD). Based on these specifications, a common set of security requirements for the operation of electronic passports has been issued as a dedicated ePassport Protection Profile, which allows Common Criteria security evaluation.

Electronic data stored on the passport's chip is protected by security measures known as Basic Access Control and by Passive Authentication, as required by ICAO. These measures ensure that the protected data cannot be read illicitly and cannot be altered. The biometric data stored is protected by the Extended Access Control protocol – this performs the BAC protocol and then runs further PKI based checks to guarantee the authenticity of the chip and reader system. However the chip also contains data that is non-protected and is designed to be openly read by anyone. It is this data that recent so called hacks have accessed.

Furthermore, the ePassport chip and embedded software provide strong countermeasures against tampering, reinforcing the non-alterability of the security features. The resistance of these features to highly likely attacks is controlled at the highest level through the Common Criteria evaluation scheme.

We recommend a renewal cycle of five years – again this corresponds to the technology cycle for Smart Security technologies.

2.2.3 National ID

National ID cards store the following assets – identity data and biometric data. In Europe, national ID cards may also be used as passports within Schengen borders. In this case and for general identification purposes, what we have written about passports applies. So once again, both the probability and impact of attack are high.

Their second use case is for accessing eAdministration and eGovernment services. Again, if a stolen card can be used by anyone, or if the identity or the biometrics stored in the card can be cloned easily, this will allow a fraudster to impersonate the owner and misuse citizen services. They may also gain access to the real owner's personal data, disclose, counterfeit and modify this data. Once again, both the risk and the impact of potential attacks are high. In this case, as well as the methods

outlined above, authentication of the owner and encryption of stored and transmitted data are the preferred means of protection.

Many countries favour a ten year or even longer renewal cycle for identity cards. Again, because of continual progress in both technology development and means of attack, we recommend a five year maximum renewal cycle.

2.2.4 Driver's licence

Driver's licences can also be used for identity checks in some countries. Again assets include identity data, and in this case driving rights, and they are at risk from unauthorised access, modification and cloning. The probability of unauthorised access and modification of data occurring are medium to high whereas the probability of counterfeiting is high. While the impact of unauthorised disclosure may be low, the impact of modification and cloning are medium to high, depending on the functionality of the driving licence.

Encryption and authentication are the type of high security protection measures needed. When the system is used for driving rights checks, the threats are unauthorised disclosure, modification of data and counterfeiting. The security measures required are encryption, authentication and firewalls, to separate identity from driving rights applications and their level is high. Renewal cycles vary considerably from ten years to never but we would recommend a five to ten year renewal cycle. If the driving licence is used as an identity card then a five year renewal cycle should be the maximum. The current recommended EU renewal cycle is ten years.

2.2.5 Healthcare

The way in which healthcare cards are used varies considerably between countries, depending on both policy and the way in which the health services are organised.

Healthcare cards may contain identity data, biometric data and in some cases medical data. There is a risk that data may be disclosed to unauthorised personnel – confidentiality is a major concern with health data.

Where healthcare cards are used mainly for data automation, the cards contain only administrative data such as patient name and social security number. Stealing or counterfeiting a card may allow a fraudster to obtain a prescription illicitly but if he has to pay for the medication anyhow, his interest is likely to be limited and so risk and probability are low. In this case basic security ensuring data integrity is sufficient. However if the medication is free to the cardholder at the point of sale, then it may be more interesting to steal cards or use the cards of relatives or friends, therefore the risk and probability rises. Additional security should be considered here - possible countermeasures include authentication, encryption and firewalls to counter unauthorised disclosure, mutual authentication and digital signatures to stop fake invoices and prescriptions and authentication and encryption to prevent counterfeiting. This is particularly important where cards are used to carry electronic prescriptions and may be vulnerable to attacks to alter the prescription data. Cards should be renewed every three to five years.

2.2.6 Basic prepaid SIM cards

Basic prepaid SIM cards are used to identify the subscriber to the network and to pay for calls. Often high value international calls are not permitted. The assets they store are the subscriber identity and network rights. Threats include cloning and stealing – hackers basically want to get free calls. The probability is high – hackers have demonstrated their abilities to make these attacks many times – but the impact is low. Network systems are set up to detect attacks and the level of the potential loss is not that significant. The security required to counter these threats is actually quite simple – a PIN code and a stronger algorithm. In particular this means not using the COMP128-1 algorithm, which has already been compromised, allowing the retrieval of keys.

Because, in contrast to higher specified SIM cards (see below), potential losses are not that high, a medium level of security is quite appropriate. We recommend card renewal every three years.

2.2.7 SIM cards

As the functionality of mobile phones increases, so does the number of use cases for SIM cards. At the same time, the job of keeping SIMs and the assets they store secure becomes much harder. In all cases these assets are the subscriber identity and network rights, but now they may also include access to other services, including payments. Use cases also vary. Those that require medium security countermeasures and are at risk from SIM cloning are making phone calls and mobile internet access. As with prepaid SIM cards, these include the use of PIN codes and stronger algorithms. It is also necessary to ensure that only trusted applications are downloaded and that individual applets are safely separated with firewalls. Once again the probability is high – hackers have demonstrated their abilities to make these attacks many times – but the impact is low. Network systems are set up to detect attacks and the level of the potential loss is not that significant.

It should be noted that what applies to GSM and 3G in these use cases also applies to CDMA and its equivalents that use Secure devices.

However in contrast to prepaid SIM cards, the further use cases on higher specification SIM cards of mobile banking and mobile TV require higher security measures and are also at risk from cloning or card modification. However mobile banking is largely equivalent to internet banking and the security requirements are similar. It is simply the channel that is different. Nevertheless for the bank and operator, the loss of image resulting from the publication of such attack would be very damaging.

With mobile TV, anyone with a genuine reader can gain access to broadcast content. Dumping the keys and rights from one card and allowing the generation of cloned cards, being able to modify the rights or reloading expired rights, will cause significant loss in revenues for the service provider as in this context the detection of a fake card is not always possible.

The probability of this is high to very high – pay TV is one of the biggest target areas for fraudsters. The impact is high for the system provider but negligible for the user. A high security level to counter these threats will include strong encryption, a secure

channel to broadcast the content, strong authentication to ensure that only trusted applications are loaded on the platform, and a secured platform resistant to high attack potential. In this case, we suggest a very short renewal cycle for cards – two or ideally one year.

2.2.8 Payment cards

When smart cards are used for payment, the asset to protect is straightforward – money, both for the user and for the system operator. Liability is also at risk but ultimately that comes back to money.

Payments can be made in closed private systems or in open banking systems. In the former case, for example cafeteria systems, only basic security is needed to protect against threats of cloning or stealing or reloading fake value because the potential value of the loss is almost always small. However in banking systems, for credit, debit or electronic purse, high security levels are needed to protect against stealing and cloning.

In fact open system payments are undoubtedly the area where public awareness of security risks is the greatest. It is also the area where Smart Security technology has had the most publicly visible impact, with the introduction in many parts of the world of the EMV (Europay, MasterCard, Visa) smart credit and debit card technology, developed by the payments associations.

Payments card technology is generally divided into three types: old style magnetic stripe and embossed technology, which is still in general use outside Europe and Asia, contact smart card technology, which is what EMV cards use and contactless smart card technology, which is increasingly being adopted for low value payments.

Fraud in the payments area either involves duplicating card details to steal money from the genuine cardholder or manipulating card details to make payment without debiting an account in any way, producing in effect the ability to create money.

Traditionally, card skimming has been a major risk for magnetic stripe cards. The information stored on magnetic stripes is straightforward to copy and duplicate with easily available equipment. This can be done using dedicated card skimming devices or point of sale terminals or ATMs that have been tampered with. The cardholder may not be aware that anything has been done until unfamiliar transactions appear on his statement.

Using smart technology allows banks to authenticate transactions as coming from a genuine card. The risk is minimised even further by using dynamic data authentication rather than static data authentication, as this means that fresh data is generated for each individual transaction by the card. Security testing procedures required by the card associations ensure that equipment meets their clearly defined security requirements.

Now, with the explosion in the use of contactless cards, especially in the US, there is concern that eavesdropping technology could be used to skim contactless cards. The earliest contactless trials in the US transmitted transaction data in the clear, fuelling this concern. However providing issuers use secure microcontroller chips, appropriate software and strong encryption, this is not a major threat. These contactless Smart Security cards are very much more secure than dumb RFID or

radio frequency devices, which are designed to transmit data openly over longer distances. In addition cards only come to life within a very short distance of the reader and the data transmitted is good for one use only.

Other potential risks include lost and stolen cards. Again, magnetic stripe cards, used without a PIN are most vulnerable to this but a smart card, contact or contactless, without a PIN could also be at risk.

This means that payments cards need PIN codes, strong authentication and strong encryption and a secure platform that can resist the high probability of attack. The EMV protocol specifies secure exchange protocols, mutual authentication of the card and terminal, online transactions wherever possible and static and dynamic data authentication.

In private systems the probability of occurrence is medium and the impact low and a renewal cycle of five years is quite adequate. In contrast, a two year renewal cycle is vital for banking systems where both probability and impact are high.

Mobile and contactless payments may be perceived to introduce additional risk to these use cases but in fact the security requirements and factors are the same as for contact.

2.2.9 Internet banking

With internet banking, once again, the assets in questions are money, both the issuer's and the operator's, and liability. This time however, the transaction is being carried out remotely and there is no straightforward way to see who is conducting it.

The main threat here is theft from the account, either using a stolen or cloned card, or through using information obtained by phishing. Another threat is the disclosure of information to unauthorised parties. In both cases the security rating is high.

Payment applications' card security measures also apply here. On top of that a strong mutual authentication protocol must be used to ensure that both the bank customer and the web site are genuine. Solutions with mutual authentication, using PIN, session keys and other OTP (one time passwords) have to be implemented. The probability and impact of threats are both high and a two year renewal cycle again is necessary.

Part 3 - Choosing the correct level of security

This paper has examined how security risks differ in different use cases for Smart Security objects. It has explained the difference between different levels of security and why it is so important to choose the correct level of security for your product and use case area. It has also shown that it is appropriate to pay more for a higher level of security and that how frequently you renew Smart Security technology can make a major difference to the security of a system.

But how do you choose the appropriate level? To help people purchasing Smart Security systems make the decision, Eurosmart has developed a self-assessment Smart Security ranking system that classifies risk levels and hence security requirements into four levels: basic, medium, high and very high.

To carry out this risk assessment for your product, please answer the following questions, carefully reading the instructions below first.

	Questions	Points			Weighting	Total
		1	3	5		
1	Is a full copy necessary for an attack or just a functional copy?				2	0
2	Potential income for the hackers from attack?				4	0
3	How quickly will the attack produce a payback?				1	0
4	How long is the lifecycle of my product?				1	0
5	How cheaply can the hacker fake or manipulate my product?				1	0
6	How much skill does a hacker need to attack my product?				1	0
7	How easily can a hacker access my sensitive data?				1	0
8	How widely available are samples of my product?				1	0
9	How motivated is the product end user to protect the product from attack?				2	0
10	Is my product also a target for ethical or recreational hackers?				2	0
11	How much will an attack damage the image of my product?				2	0
12	If my product is successfully attacked how much will this damage my company?				2	0
					Risk total	0

Before answering each question, please read the question notes below and then enter a rating into the table – 1 for low, 3 for medium and 5 for high. Then multiply that rating by the weighting factor for the question and enter the answer into the total column. For example, if your answer to question 2 is medium, enter 3 into the table, multiply 3 by the weighting factor of 4 to get 12 and enter 12 into the total column for question 2.

Once you have answered all the questions, add up your totals to obtain your total vulnerability rating. Check this figure against our scale to see whether you should be using basic Smart Security, medium Smart Security, high Smart Security or very high Smart Security.

75+ very high Smart Security
55-74 high Smart Security
35-54 medium Smart Security
17-34 basic Smart Security

1 Is a full copy necessary for an attack or just a functional copy? Does the fake Smart Security object need to look like a genuine object in order for the attack to succeed or not? If attacks are carried out in public, the answer may be yes. If not, then the answer may be no. It will require more effort on the part of the attacker to create a full copy. Score 1 if a full copy is needed and 5 if a functional copy will suffice.

2 Potential income for the hackers from attack? How big is the financial motivation for the hacker to carry out the attack? Remember to consider this at the system level and not at the level of the individual Smart Security object. If the overall payback is low, score 1. If it is medium, score 3. If it is high, score 5.

3 How quickly will the attack produce a payback? If the attacker can produce a worthwhile payback in a short period of time, score 5. If the attack takes a long time to carry to fruition, score 1. This shows why a short renewal cycle for your Smart Security technology can be a good investment – it may make lengthy attack development less worthwhile for the fraudster.

4 How long is the lifecycle of my product? If your product lifecycle is short, score 1. If it is long or if the product is updated rarely, score 5 – this allows the attacker more flexibility and time in developing his attacks.

5 How cheaply can the hacker fake or manipulate my product? Attacks that require expensive, sophisticated equipment will be less attractive to some hackers. If expensive equipment is required, score 1. If attacks can be carried out with equipment available to anyone, score 5.

6 How much skill does a hacker need to attack my product? How technically skilled does an attacker need to be to carry out a successful attack? If any engineer could do it, score 5. If extensive specialist knowledge and training is needed, score 1.

7 How easily can a hacker access my sensitive data? How widely available is information about how to carry out an attack or which helps the hacker in carrying out the attack? For example is there a master key that is available on all cards? Or does each card carry an individual key If it's easily available on the internet or elsewhere, score 5. If it is harder to obtain, score 3. If it is unavailable to outsiders, score 1.

8 How widely available are samples of my product? Can a hacker easily obtain copies of your Smart Security technology to perfect his attack? Are freely programmable products available to purchase? If yes, score 5. If no, score 1.

9 How motivated is the product end user to protect the product from attack? Does the end user take good care to protect the product (for example bank cards)? Or will he lose nothing and maybe even gain from a successful attack (for example Pay TV cards)? Issues to consider include whether the product helps the consumer protect him or herself from fraud, identity theft or theft of personal data or rights and whether the consumer is aware of that and values it. If he protects the product carefully, score 1. If there is a potential for the user himself to become the attacker, score 5.

10 Is my product also a target for ethical or recreational hackers? Even if there is little potential financial benefit to a successful attack, some attackers may be motivated by prestige or ethical concerns, increasing the potential for attacks on your product. If yes, score 5. If no, score 1.

11 How much will an attack damage the image of my product? If an attack could seriously affect the image of your product in the marketplace, score 5. If not, or if attacks are unlikely to become public, score 1.

12 If my product is successfully attacked how much will this damage my company? What is the potential financial damage of an attack to your company? If it could potentially cripple the entire company, score 5. If the risk is only to a single product line and will be insignificant overall, score 1.

In the future Eurosmart members selling Smart Security may also use these criteria to describe the security of their products. To support this industry rating of products, Eurosmart has adopted a new label of 'Smart Security' that should be associated with this list of criteria and the definition of security levels. The purpose is to give an idea of the value of the product (in terms of security) behind the label.

Basic, medium and high levels will be self-awarded. A grading of very high for a product must be checked and endorsed by Eurosmart. The award of a level can be represented by an exclusive Eurosmart graphic.

Part 4 - Conclusion

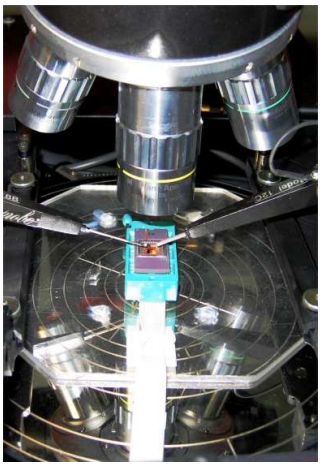
From looking at the different use cases for Smart Security objects and from considering the different type of attacks and risks that exist, it is clear that it is vital to choose the appropriate level of security for a system. The Eurosmart ranking system can help you do this, providing you have a sound understanding of the risks associated with your particular risk case. Of course you should treat this as a guideline – it does not replace thorough consultation with a qualified vendor. It is your own responsibility to ensure that you provide adequate protection for your system and assets.

Nonetheless, chosen correctly, with a sound understanding of the right renewal cycle, Smart Security objects from a reputable supplier are cost effective tools that can protect against all types of attack, from the most simple to the most advanced. As the securest element in the chain, Smart Security objects are the cost efficient way to protect assets. They allow you to select the right amount of security for the right price.

Of course you get what you pay for. Higher security Smart Security products will cost more than lower security objects. However, that added cost is an investment in system security, reliability and trust that will pay off in terms of ease of operations, customer service and public relations – all vital factors that are put at risk by not buying the appropriate level of security.

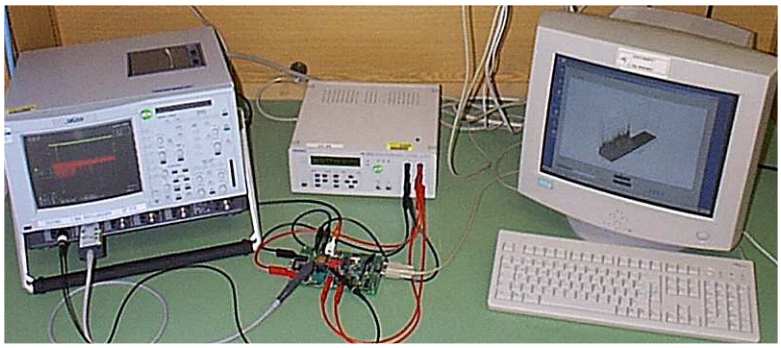
Attack methods and equipment

Physical or manipulative attacks



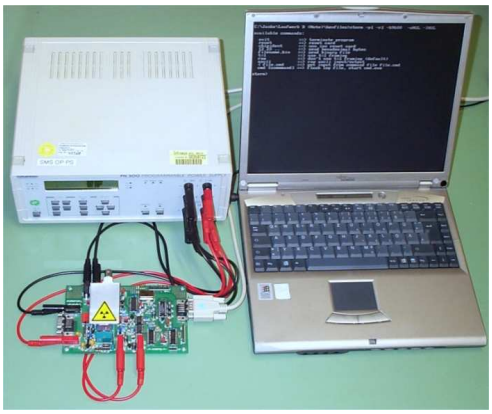
Manipulating attack: Smartcard IC with probing needles at a probing station

Observing attacks



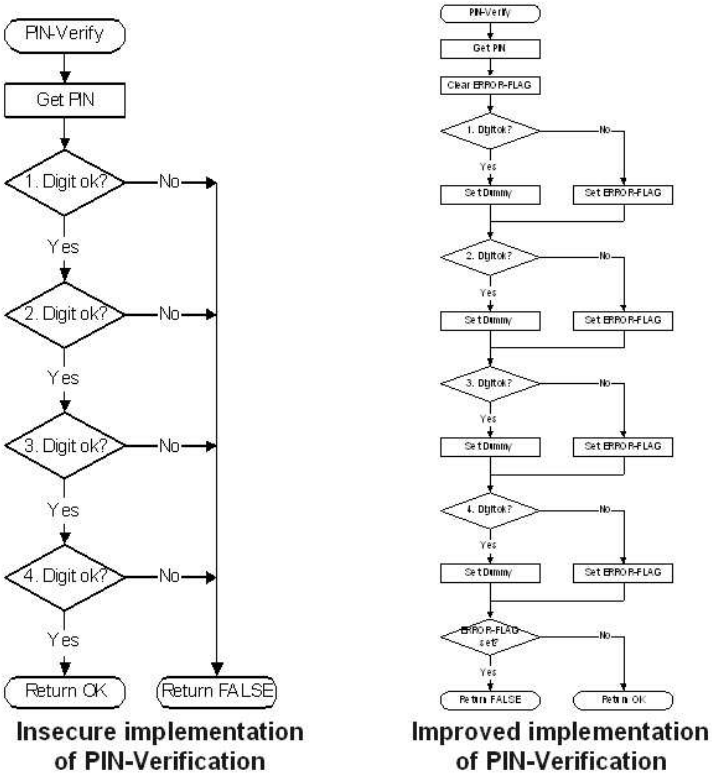
Lab setup for performing observing attacks like power analysis

Semi invasive attacks



Semi-Invasive/Fault Attack in Lab using alpha particle on a smartcard IC

Logical attacks

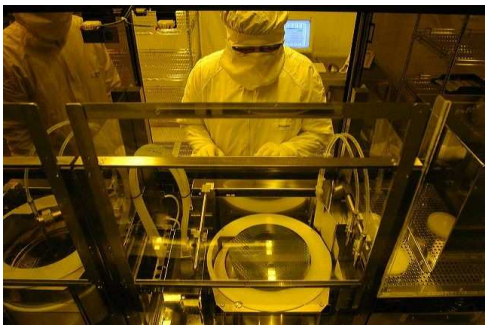


Insecure and improved realisation of PIN verification

Applications and security

Cloned SIM-cards

General security hardware



Test of smartcard ICs (every chip is tested before shipment - including also some basic security mechanisms)

Eurosmart is an international non-profit association located in Brussels and representing 25 companies of the smart security industry for multi-sectors applications. Founded in 1995, the association is committed to expanding the world's smart secure devices market, developing smart security standards and continuously improving quality and security applications.

Manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators, application developers and issuers gather and work into dedicated working groups on communication and marketing, security, electronic identity and new form factors, and prospect emerging markets. Members are largely involved in political and technical initiatives as well as research and development projects at the European and international levels

Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry".

More information: www.eurosmart.com

EUROSMART
Rue du Luxembourg 19-21 – B-1000 Bruxelles
Tel. (+32) 2 506 88 38/ Fax. (+32) 2 506 88 25
Email : eurosmart@eurosmart.com