Security and Privacy in the Digital World

Solutions from the Smart Security Industry

Digital Security Reference Paper

Content

June 2012

1. Executive Summary

Do you feel confident when you make a payment with your smartphone? Are you concerned that your digital identity could be stolen and that illegal use could be made in your name? Do you worry about who could access your personal data stored in the Cloud?
Few people are indifferent to these questions, which is why Eurosmart has attempted to give some answers in this digital security reference paper and in three related documents.[1]

While there is little need to point out the importance of digital information and processes for a modern and innovative Europe, it is critical that our digital society is protected from malicious human activities. We are reminded of this fact every time there is a major data breach, and confidential information like credit card details is exposed by hackers. The digital security industry has developed solutions for identification, authentication, access control and digital signature, used for services like mobile telephony and electronic payments. Smart secure solutions use features such as tamper resistant hardware, secure embedded software, cryptography and security protocols that address challenging concerns such as data confidentiality and integrity, authentication, privacy, non denial of service, non repudiation, digital content protection. But what are the methods and technical skills required to build these solutions? How can we manage the balance between the need for security and its cost in term of performance and resources? Is there a way to guarantee effective security and to rank the level of security of different solutions?
This paper tries to answer these questions and explains how solutions based on smart secure devices are essential in achieving very high levels of protection against threats in an unsecure environment.

2. Introduction – Purpose of this Reference Paper

The objective of this digital security reference paper is to explain what digital security means and how it is achieved and evaluated.
As regards of security, the manufacturer's claims are not sufficient to gain the confidence of the consumer. The elements constituting the chain of trust from the threat inventory to the security certification must be explained. This paper provides an overview on the methods and techniques that are used to build and to assess solutions to answer the security threats with a focus on solutions based on smart secure devices, such as smart cards and smart tokens.

Digital security gives individuals and organisations the freedom to embrace the digital lifestyle. It equates to the protection of their identity, their personal data and assets, as well as their technology means when they use digital devices and networks (private, public, Internet and mobile) and use cases such as communication on a social network, financial transactions, e-administration and e-commerce.

In this perspective, security is different from:

- Safety, which is the state of being protected against unintentional harm events;
- Reliability, which is the ability of a device to perform its functions while being protected against failure of a component;
- Quality, meaning the avoidance of issues stemming from defects.

[1] Security of Mobile Devices, Applications and Transactions (Eurosmart, 2012)
Smart Embedded Security for the Internet of Things (Eurosmart, 2012),
Access Management as a Subset of Privacy and Security in Cloud-Based Services (Eurosmart, 2012)

Security pertains to the protection against threats that are related to malicious human activities.

Now, just like in the case of physical security measures, digital security solutions must be chosen in accordance with the level of threat and its potential harm. Effective security only results when there is a correct trade-off between the level of security measures and the convenience of these security measures.

As an example, user name and password may be fine for authentication to a subscription-based news service on the Internet, but it is not appropriate for accessing online banking services.

Digital products or systems must perform their functions while exercising proper control over the information so as to ensure it is protected against hazards such as unwanted or unwarranted dissemination, alteration, or loss. Additionally, individuals have a reasonable expectation that their personal information contained in digital devices or systems remain private, be available to them as needed, and not be subject to unauthorised modification.
Digital security should protect against the following (non-exhaustive) list of threats:

- Identity theft, for illegal immigration, terrorism or financial gain;
- Fraud in financial transactions or commercial transactions, for financial gain;
- Infringement of intellectual property rights and copyrights, to obtain social benefit;
- Confidentiality breaches, for gaining competitive advantage or commercial exploitation;
- Intrusion in digital systems, introduction of viruses, Trojan horses, malware and botnets aiming to destabilise an organisation;
- Destruction of data, theft of data or malicious modification of data for fun or vandalism.

Eurosmart, “the voice of the Smart Security Industry” brings together leading actors worldwide that develop products and solutions for digital security. In this paper, we examine civilian security in the private / public domain and are thus excluding defence, aviation and aerospace.

The digital security industry has developed solutions using tamper resistant hardware, secure embedded software, cryptography and security protocols that address challenging concerns such as data confidentiality and integrity, authentication, privacy, non denial of service, non repudiation and digital content protection. Some security services as identification, authentication and digital signatures have also been standardised.

These features are implemented by software, but smart secure devices such as smart cards or secure elements are essential in achieving very high levels of protection against threats. Smart secure devices embed a secure microcontroller that is both a “safety deposit box” of data and processes and the support base of embedded software that cannot be subject to viruses, malware or Trojan horses. The process of personalisation of a smart secure device is also securitised. And finally, a smart secure device is personal and portable, so under its owner’s control.

Eurosmart members design products and solutions whose level of security can be evaluated and certified by independent laboratories and certification bodies utilising experienced methodology and internationally recognised standards.

3. Security Issues... and their Solutions

3.1 Security Risk Analysis

A security risk analysis determines the effect of and condition for a successful attack related to the application to be protected. For example, what happens if my credential in my electronic passport is known (Can someone else use my identity? Could it be used by a terrorist?). The solution selected to secure the application will depend on the value of the asset to protect.
An asset is information that could mean money (i.e. protecting money inside a smartcard epurse), intellectual property (i.e. a software element loaded inside a memory component), credential (i.e. private information inside an electronic passport), etc.
Hackers or malicious users are motivated by various considerations and deploy technical means to abuse the functionalities of a device. Legal penalties are good barriers, but are not sufficient to limit the scopes of attacks.
Risk analysis enables the identification of the threats that place the assets at risk. Risk mitigation consists of the introduction or addition of security measures with the aim of reducing the risk. The security measures may be applicable to the product itself as new security functionalities or to its operational environment. For instance, in the risk assessment, where and how an element of digital content is stored is highly important (i.e. a computer protected by a strong firewall inside a bunker, or a system that is accessible to anyone, such as an electricity meter).
But security is never absolute, we can have surprises through the fact that some threats were not taken into account or badly estimated.

It has also to be noted that it is much cheaper and easier to implement the right level of security when designing a system rather than trying to increase the security level of an existing system that has been defeated. This is often referred to as the Security by Design principle.

Security experts possessing state of the art knowledge of attacks and countermeasures need to be involved in thoroughly studying user requirements, evaluating risks and proposing solutions based on the best trade-off in term of security, cost and performance.

3.2 Attacks and Tamper Resistance

For IT products, substantive standardised presentations of potential software vulnerabilities and attack methods have been published in the form of the Common Weakness Enumeration (CWE™)[2] and the Common Attack Pattern Enumeration and Classification (CAPEC™)[3].
Embedded systems, such as smartcards, operating in a public environment can be submitted to a great number of attacks. They are enumerated in a publicly available document drawn by an international community of smart security experts[4] and briefly summarised hereafter:

i/ **Non invasive attacks:** the attacker will try to find a mode where the system is not strong enough or he or she will try to bypass some security mechanisms without damaging the system. These attacks may be very efficient and usually do not require sophisticated equipment:
With **software attacks**, the attacker will exploit vulnerabilities in protocols, crypto algorithms, or in their implementation.

[2] http://cwe.mitre.org

[3] http://capec.mitre.org

[4] Common Criteria supporting documents: CCDB-2009-03-001-Application of attack potential to smartcards V2-7

With **side channel attacks**, the attacker will monitor and perform analysis on the system power consumption, timing, electro-magnetic field emission and radiation, and use the information leakage to retrieve sensitive data.
With fault injection attacks the attacker will use abnormal environmental conditions to create an uncontrolled behaviour of the system. Environmental conditions include but are not limited to voltage, frequency, temperature, signal glitches, light electro-magnetic fields and radiation)
ii/ **Invasive attacks:** the attacker will break into the system (reverse engineering, Microprobing, FIB, e-beam..) to modify or clone it. In general, these attacks require sophisticated equipment from the semiconductor industry and a deep knowledge of semiconductor and secure firmware.

Products that are resistant by themselves to all these attacks are called “tamper resistant” products.

3.3 What are the main Security Functions?

The objectives of digital security are:

- to securely authenticate an object or a person,
- to securely store data,
- to securely transfer information from point A to point B,
- and to securely execute applications.

A system will be made secure by using one or a combination of these techniques to address to the following kinds of issues:

- Authentication: Am I communicating with the right device/person? Can I trust this device/person?
- Data protection: Who can access my personal/confidential data? Is the data accurate? Has the data been modified?
- Secure Communication: Can a third party read the information I send? Can a device accept a command from a host? Can I trust the information I receive?
- Trusted Execution: Can I trust the application I am using? Is it running in a safe/trusted environment?

To securely authenticate, store, transfer or execute information, cryptography techniques are used in combination of security expertise (to overcome attacks listed in the previous section).
The three basic functions of cryptography are:

- Authentication (signature): to establish true identity, to detect fakes;
- Encryption: to keep information secret, to prevent data theft;
- Data Integrity (Hashes) - Detecting changes so as to prevent illegal modifications.

These functions are built from cryptographic algorithms, which are the “basic building blocks”. Some of these algorithms use “secret key” mechanisms: a secret is shared between point A and point B in order to communicate in a secure mode. It is a very efficient mechanism, but the security is compromised if the secret is disclosed. DES 3DES and AES algorithms are the most common ones used in the industry.

Other algorithms use private/public key mechanisms: secure communication can be established without sharing of secrets. These techniques are extremely efficient, but require quite a high level of computing power. RSA and Elliptic Curves are the most commonly used versions today.
Most applications combine both types of algorithms to perform the cryptographic function e.g. exchanging secret keys for a DES using private/public RSA algorithm.
Sometimes, cryptographic mechanisms can be compromised by using massive computational power. The strength of the mechanisms depends on the parameters of the algorithms such as the key lengths. Here too, a trade-off must be found between security and performance.

With the right parameters, some standard algorithms are considered to be trusted and robust against brut force attacks because they have been in depth analysed and thoroughly tested. The use of proprietary algorithms is risky (security by obscurity), as it may have theoretical or actual security vulnerabilities. If those vulnerabilities are exploited, the overall system security can be jeopardized.

A careful management of the keys and their protection is of the greatest importance. When a key is disclosed, the door to the critical assets is wide open. For this reason, a hierarchical system of keys may be built, where the bottom level keys are widely distributed in the system and at the top level, the master key is strongly protected in a unique place. In this case, the disclosure of a basic key gives only a limited access to assets, and attacks are thus confined to a small portion of data.

Authentication

There are several ways to authenticate objects or persons. It may be through something you have (i.e. a smart card or a USB token), something you know (e.g. a password or a PIN code.) or a unique personal trait (i.e. a finger print or iris scan) and obviously again, a combination of these techniques.

Authentication of a machine is obtained thanks to a cryptographic protocol.

Data protection

While data are protected during their manipulation by a trusted execution and during their transfer by secure communications, stored data must also be protected.

There are several ways of storing information on a medium: magnetic strip, hard disk, and a great variety of memory devices offered by the semiconductor industry: ROM, RAM, EEPROM, FLASH, etc. Storing resources can be locked in a safe room but for devices that are running in an unsecure environment, the stored data must be protected by the device itself.

Some technologies are intrinsically more secure than others (e.g. a ROM memory, written in binary elements during the silicon manufacturing process of a chip vs. en embossed information on a plastic card, laser engraving or holograms). Scrambling of the memory addresses and encryption of the memory content enhance the protection level.

In any case, the access to the data must only be provided to authorised persons, machines or processes. Access control to the storage resources in accordance with a predetermined security policy (i.e. Who is authorised to access what, and under what conditions?) is a basic security function that can be found in the hardware and at all levels of software.

Secure communications

Secure communication begins with the authentication of the communicating parties. Then the integrity of the communication is guaranteed through the proper management of the sequence of the exchanges and by checking the integrity of the content in the exchanges. Confidentiality is encrypting ensured through the encryption of all or part of the data exchanged. Various secure protocols have been designed and standardised for use in different communication layers. They are built on cryptographic functions such as CRC, hash messages, signature, MAC, etc., which assure such properties as authenticity, integrity and confidentiality as well as non-repudiation etc.

Integrity and confidentiality may be also assured internally when the data is moved between the memory and processing engine via hardware, implementing basic cryptographic mechanisms.

Trusted Execution

Execution can be trusted when:

- it is done on behalf of an authorised user;
- the flow of instructions that commands the execution is not corrupted;
- the right data is manipulated;
- there are no flaws that can be exploited to obtain a different result than that which is expected;
- there are no leaks of sensitive information from one context of execution to another.

An application that needs to be executed securely must first simply comply with its own specifications, including the required security controls. The application requires primitives and relies on operating systems that offer reliable security services, in particular isolation between applications. These services must themselves be securitised by countermeasures and may use security options offered by the hardware such as MMU, system mode and exception handling. It is not enough to detect the induced errors, but the software must also react with appropriate operations to place itself in a safe mode and protect the sensitive data.

Smart devices are built according to these principles and rely on hardware that provides at least secure storage. Tamper resistance is obtained by an adequate combination of software and hardware security features

A smart device can also be used as a trusted bootstrap. It is the first component to start and can be considered as a trusted seed. The function of this seed is to check the reliability and availability of all the different components, verifying their authentication and guaranteeing the integrity of the data they contain.

Trusted Execution Environment (TEE) is a technology which brings a different execution context beside a classical system and may share the same hardware resources. It ensures the protection against software attacks compromising the classical system.

3.4 Key Qualities of a Secure Product

Correctness and Robustness: A secure product must behave as described in its specification (correctness) in such a way that weaknesses not been introduced in its implementation. And this, whatever the environmental conditions may be (robustness), in order to be resistant to attacks;
Predictability: A secure product must have a fixed and pertinent behaviour in response to an attack;
Sensitivity: A secure product must be able to distinguish an attack from a disturbance due to a “noisy” environment;
Durability: The evolution of state-of–the-art of attacks must be anticipated at the moment of designing the product;
Soundness: Development, manufacturing and delivery must be undertaken under strict control, guaranteeing that traps, viruses, Trojan horses, malicious code or exploitable errors cannot be introduced.

3.5 Security Measurement

A product or a system may be protected by the environment and / or by embedded technical measures.
Security provided by the environment may be specified and evaluated following some standards such as ISO/IEC 27000. This aspect is out of the scope of this paper.

However, an evaluation of the embedded technical security of product or a system can be done in regard of multiple criteria:

- Suitability of the security measures with regard to the threats;
- Correctness of the security measure implementation;
- Strength of the security mechanisms (password, pin, cryptographic algorithms, etc.)
- Resistance against attacks that are designed to circumvent or break the security measures.

Measuring security is fundamental to offering all stakeholders a high level and easy-to-read security classification. For this purpose, several security standards have been initiated, the most famous being the Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC)
There are also national security standards such as FIPS 140-2 from US authorities, CAPS & CPA certification schemes from UK authorities, the CSPN certification scheme by the French authorities, the ZKA certification by German authorities etc.

Apart from these international or national standards, private security schemes have been defined with a restricted applicative scope. This is the case in banking applications, where Visa, Mastercard, American Express and other financial institutions, as well as groupings of them such as EMVCo or the PCI Security Standards Council, have developed specific functional and security certification schemes.

3.6 Common Criteria

Common Criteria

Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is registered as an international standard: **ISO/IEC 15408**.

About 1600 CC certificates have been issued, with a third of these delivered for smartcards and similar devices.
A certificate qualifies a Security Target, which is specific to a product and compliant to a Protection Profile (PP).
A PP is a generic specification identifying security requirements for a class of security devices (i.e. a secure signature creation device).
Common Criteria provides a catalogue of security assurance requirements concerning the specification, design, implementation, testing, life cycle management and development environment. In addition, a specific class of assurance concerns vulnerability assessment supported by penetration testing.
The assessment of a product with regard to the security requirements is summarised by the Evaluation Assurance Level (EAL). Each EAL from 1 to 7 corresponds to a set of security assurances covering the complete development of a product, with an increased level of strictness and effort for the developer and the evaluator.
The level for smartcards and similar devices is never less than EAL4 +, where + pertains to the highest level of resistance (noted AVA_VAN.5 on the certificate).

Smartcards and similar devices operate in hostile environments and the target is available to attackers for physical attacks to the hardware. With the claim of the highest level of resistance against attacks, the chip shall be included in the scope of the evaluation and the penetration tests include all kinds of tampering attempts and analyses of information leakages from the various side channels. CC certification with these conditions guarantees the tamper-resistance.

A CC certificate has no limit in time and it is up to the risk manager of the product to take care of the attack state of the art upgrading. But a reassessment could be done upon the demand of the developer in order to reset the date of certification issuance. A regular reassessment is also required when the target of the certification enters as a component in a product to be evaluated. And finally, certified products are updated by the issuer at regular product reissuance intervals.

Evaluation of a product is led by an independent licensed laboratory under the control of a national Certification Body. It results in a Certificate and a Certification Report issued by the Certification Body, claiming the Evaluation Assurance Level and the compliance to a given Protection Profile.
With the Security Target of the product, this information is publicly available on the Common Criteria portal[5].

The Mutual Recognition Agreement (MRA) signed by 26 countries created a uniform international scheme where certificates up to EAL4 are recognised. Each certificate bears the following stamp:

A specific European agreement (SOGIS) reinforces this, enabling recognition up to EAL7. Certification bodies from France (ANSSI), Germany (BSI), Netherlands (NSCIB) and the UK (CESG) are the only ones able to issue such high level certificates accepted by other European countries.
The following logo is printed on such certificates:

[5] http://www.commoncriteriaportal.org

3.7 FIPS 140

FIPS 140 was issued in the United States of America by the National Institute of Standards and Technology (NIST) to coordinate the requirements and standards for cryptographic modules.
FIPS 140-2 evaluation is required for the sale of products to the US Federal Government that implement cryptography, but are occasionally also required by financial entities or the private sector.
The standard defines the security requirements that must be satisfied by a cryptographic module that is integrated in an IT system.
A security policy provides a description of the cryptographic module and the security behaviour it enforces. It addresses security requirement classes such as specification, interfaces, roles & services, finite state model, key management, self-tests and design assurance and specifies the level of each class. Each assertion belonging to a class required a response and an evaluation procedure to ensure that the assertion is met.

There are four levels of security: from Level 1 (the lowest: approved algorithms and functions, no physical security mechanisms) to Level 4 (the highest). The evaluation is mainly focused on the design of the module and on the validation of the algorithms, but the resistance assessment is not supported by sophisticated penetration tests.
FIPS 140-2 does not guarantee that a module conforming to the standard requirements is robust, but it is a way to enhance confidence, trust and credibility.

FIPS 140-3, the proposed revision of the standard, is only in a draft version at the moment.

FIPS 140 validation certificates specify the exact module name, hardware, software, firmware, and/or applet version numbers.
A certified crypto module is listed on the NIST web site[6]. The product is clearly identified and its security policy is available.

3.8 Private Security Schemes

Among privative security schemes, those related to payment applications are the most famous.
As a prerequisite to being used in a payment network, smartcards must be certified as compliant to the functional and security requirements required by the payment network operator (i.e. Visa, MasterCard, etc.).
A specific programme for security assessment is defined, where the process is under the full control of the operator. It monitors the attack state of the art and defines the security requirements in line with its strategy and risk management policy. Most often, security guidance for the design of the product is provided to the developer and an independent but accredited laboratory evaluates the compliance of the product to these requirements. In particular, the laboratory carries on penetration testing in order to assess the product vulnerabilities.
In some cases, the results of a CC evaluation are considered as a valid input by the private scheme. A certificate is delivered for a limited period of time and may concern the chip, operating system and application.

[6] http://csrc.nist.gov/groups/STM/cmvp/index.html

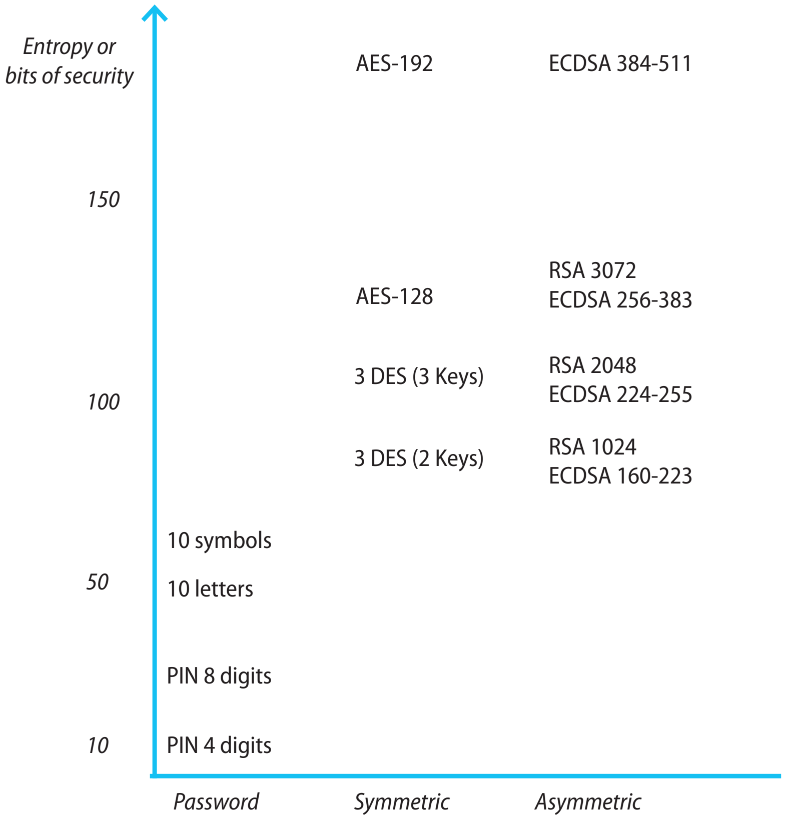
The operator's security requirements, list of certificates and products to which they relate are not publicly available.

This brief overview shows that various schemes are currently available to assess the security of a product. These schemes are attached to the validation of compliance to security specifications and to good development practices, but with different scopes and interests for robustness. Certification of smart secure devices may target the IC alone, or a combination of hardware and software or the complete device sometimes including the card body. Most often, the choice of a scheme and of the certification scope is determined by a regulation or by the market. Even if a security certificate is not an undisputable proof of protection against any threat, it brings trust in the security provided by a product.

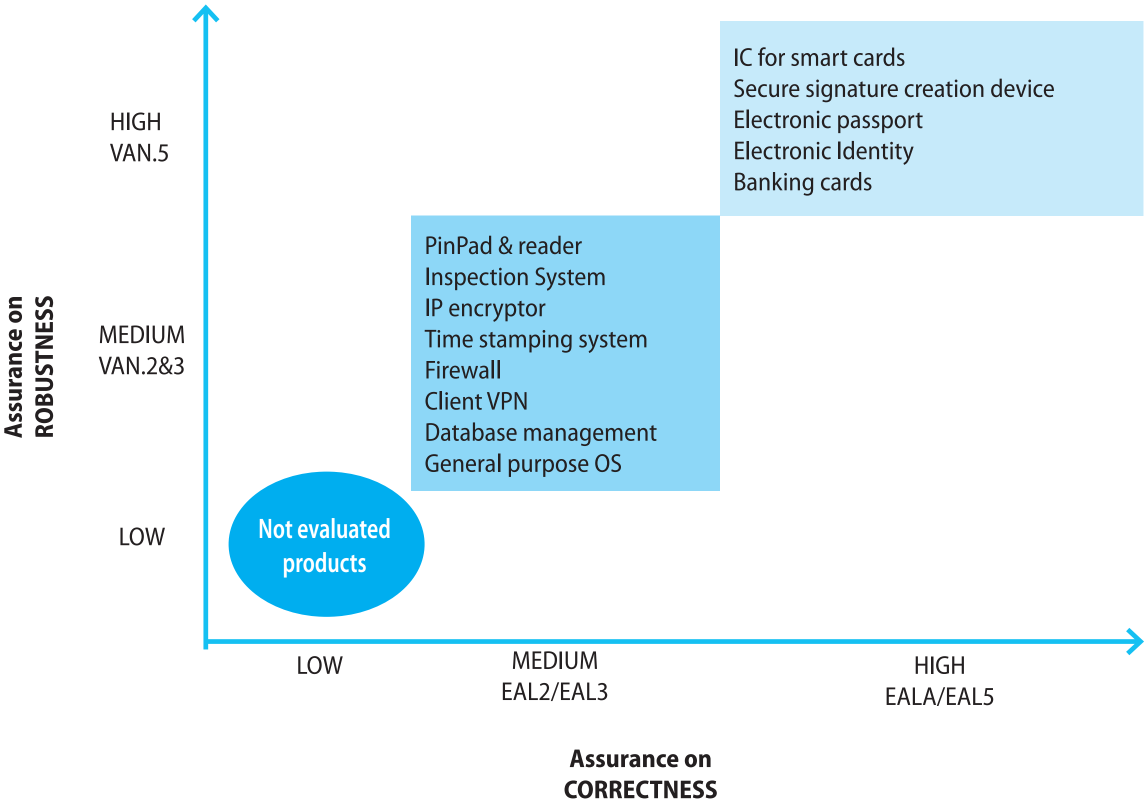
3.9 Ranking of digital Security Products

As explained above, it is not possible to give one and only one level of digital security of a given digital product or system because this is always relative to the kind of envisaged threats in one hand and depending on the quality of this design in the other hand.
This quality of the design can be represented along the three axes of strength of the mechanisms, correctness and robustness of the implementation.

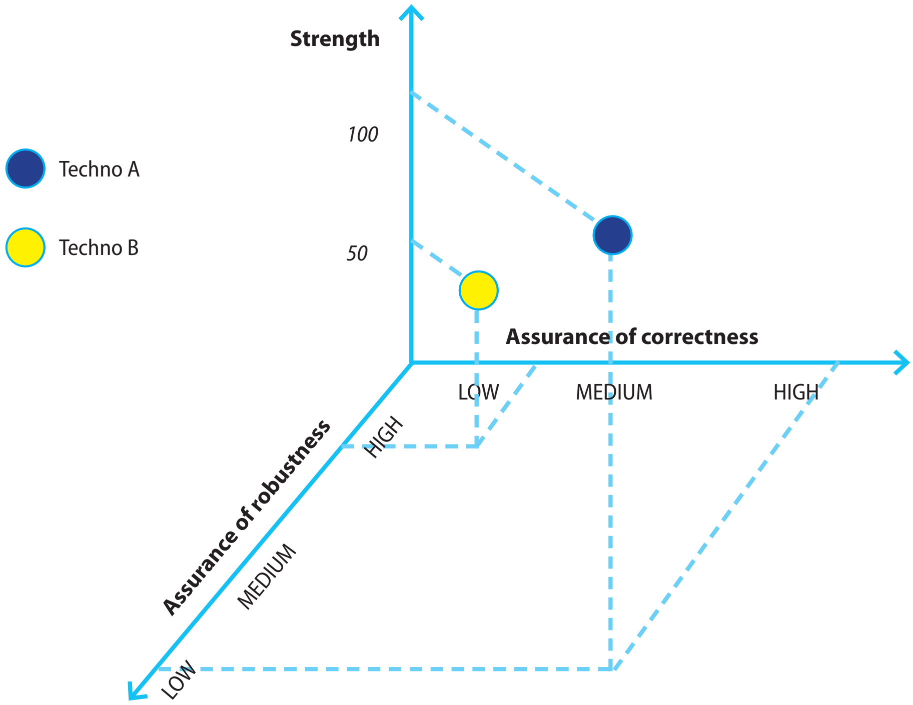
The strength of mechanism expresses the minimum efforts assumed necessary to defeat the security behaviour. It represents the chance to obtain the secret by random trial and is noted in term of entropy or bits of security.
The following chart provides an overview of the strength of password and algorithms.



Correctness and robustness of a given product must be evaluated and tested relatively to agreed standards. CC Protection Profiles allow for a comparison of the requirements for various types of products.



In this way, the realisation of a security function integrated in a product can be compared for different technologies.



4. Conclusion

We have shown how security issues of a system or a device can be analysed and treated, which security services can be offered, what the elements are that contribute to the realisation of a sound and secure design and how some assurances can be obtained thanks to security evaluation and certification. We have also presented an approach that allows for the ranking of products and technologies in a multi-criteria scale.

In this approach we notice that even if absolute security doesn't exist, smart secure devices offer vendor independent guarantees of the highest level of security. They embed powerful cryptographic mechanisms that support a wide range of security functions and are able to resist the highest attack potential in an unsecure environment. Being tamper resistant, an attacker can try any manipulation of the device he wants without breaking its security properties. Assurances on the correctness and the robustness of the security functions can be obtained from security certification and this reinforces the confidence of the customers and users in secure digital products.

5. Glossary

AES: Advanced Encryption Standard

CAPEC™: Common Attack Pattern Enumeration and Classification

CAPS Certification : CESG Assisted Product Scheme with CESG means for Communications-Electronics Security Group

The CAPS Service provides verification of Cryptographic products to UK Government standards and formally approves their use by Central Government and the wider public sector

CC: Common Criteria

CPA Certification: Commercial Product Assurance

Commercial Product Assurance is CESG's approach to gaining confidence in the security of commercial products. Assessment of products will be done against published security characteristics.

CRC: Cyclic Redundancy Check

CSPN: Certification de Sécurité de Premier Niveau (Fr)

CWE™: Common Weakness Enumeration

DES: Data Encryption Standard

EAL: Evaluation Assurance Level

EEPROM : EEPROM (also written E2PROM and pronounced «e-e-prom,» «double-e prom,» «e-squared,» or simply «e-prom») stands for Electrically Erasable Programmable Read-Only Memory and is a type of non-volatile memory used in computers and other electronic devices to store small amounts of data that must be saved when power is removed, e.g., calibration tables or device configuration. (Source Wikipedia)

EMVCo: EMVCo, LLC, was formed in February 1999 by Europay International, MasterCard International and Visa International to manage, maintain and enhance the EMV™ Integrated Circuit Card Specifications for Payment Systems. EMVCo's primary role is to manage, maintain and enhance the EMV Integrated Circuit Card Specifications with the objective of to ensure ensuring interoperability and acceptance of payment system integrated circuit cards on a worldwide basis.

FIB: Focused Ion Beam

Flash: Flash memory is a non-volatile computer storage chip that can be electrically erased and reprogrammed. It was developed from EEPROM (electrically erasable programmable read-only memory) and must be erased in fairly large blocks before these can be rewritten with new data. (Source Wikipedia)

Hash: A cryptographic hash function is a hash function, that is, an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded is often called the «message,» and the hash value is sometimes called the message digest or simply digest. (Source Wikipedia)
The ideal cryptographic hash function has four main or significant properties:

- it is easy to compute the hash value for any given message
- it is infeasible to generate a message that has a given hash
- it is infeasible to modify a message without changing the hash
- it is infeasible to find two different messages with the same hash

IT: Information Technology

MAC: Message Authentication Code

MMU: Memory Management Unit

MRA: Mutual Recognition Agreement

PCI Standard: Payment Card Industry Standard

PP: Protection Profile

RAM: Random Access Memory

ROM: Read Only Memory

RSA: RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978. (Source Wikipedia)

SOGIS: ”Mutual Recognition Agreement of Information Technology Security Evaluation Certificates – Version 3.0”, or the SOGIS-agreement is an agreement between some Europeean nations with membership in the EU or EFTA concerning mutual recognition of evaluation certificates after ITSEC or the CC standards.

TEE: Trusted Execution Environment

Authors

Alain Boudou
Didier Chaudun
Detlef Houdeau
Benoît Makowka
Christian Vignes

Legal Disclaimer

While all efforts have been made as to accuracy and pertinence of content and data contained in these documents, neither Eurosmart nor its associates may in any case be held responsible for the consequences, whatever their nature may be, that may result from the interpretation of this data or content, or any eventual errors therein.

Any reproduction of the content may only be undertaken under the strict guideline that any article used (or part thereof) be cited as follows: “source: Eurosmart”.

The inclusion of all texts, photographs and other documents supplied herein imply the acceptance by their authors of their free publication therein.

About Eurosmart

Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multi-sector 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 of security applications.

Members are manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators, application developers and issuers who work into dedicated working groups (communication, marketing, security, electronic identity).

Members are largely involved in research and development projects at the European and international levels.

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

Eurosmart members are companies (Austria Card, EM Electronic Marin, FNMT-RCM, Gemalto, Giesecke & Devrient, Infineon Technologies, Inside Secure, LFoundry, Morpho, NedCard, NXP Semiconductors, Oberthur Technologies, Prooftag, Renesas Electronics, Samsung, STMicroelectronics, Toshiba), payment systems (GIE Cartes Bancaires, Mastercard), laboratories (CEA-LETI), research organisations (Fraunhofer AISEC), associations (Smart Payment Association, Mobismart, Danish Biometrics) and independent experts (Michel Koenig, Jonas Andersson).

EUROSMART
The Voice of the Smart Security Industry

Contact us:

EUROSMART
Rue du Luxembourg 19-21
B-1000 Brussels
Tel. (+32) 2 506 88 38
Fax. (+32) 2 506 88 25
Email : eurosmart@eurosmart.com
Visit our website www.eurosmart.com