EUROSMART
The Voice of the Smart Security Industry

White Paper
Smart USB Token

April 2008

INDEX

Message from Jacques Seneca, Chairman of Eurosmart

Eurosmart evolved from the Smart Cards to the Smart Security, why?

In today's digital world what needs to be developed is an enhanced security level to perform our transactions in a safe way and strong and convenient tools to protect our privacy. At Eurosmart, we believe that the technologies coming from our industry are the rights tools to provide both.

For over a decade, Eurosmart has been promoting the usage of the Smart Cards. We believe that they are an excellent form factor to perform strong authentication and privacy management but other form factors are also convenient to perform other additional tasks: e-Passports for example, which can cope with the conventional world infrastructure constraints or USB Tokens to provide additional mass storage capabilities and convenient connectivity are also excellent solutions to host our Smart Security Technologies.

That's why Eurosmart launched recently a Working Group on this topic. This Working Group already published some market analysis and statistics for our members and it is today our pleasure to issue this White Paper which introduces the concept of "Smart USB Token", gives its definition and presents the various markets it will address.

Eurosmart will continue its efforts to show how to best make use of Smart USB Tokens, how to implement them and the main items to pay attention to when deploying Smart USB Tokens.

Enjoy your reading.

Jacques Seneca
Chairman, Eurosmart
24th April 2008

1. Introduction

During Eurosmart research for the 2020 Vision Paper, we noticed a high level of expectation from consumers and citizens for more secure and personalised tools to protect their interactions with the digital world, especially through the PC.

In a connected world, markets are driven by a need for strong authentication and for convenience.

We also pointed out a consensus among the security conscious industry that passwords are not sufficient any more, and there is a growing expectation from organisations like Banks, Governments or Enterprises for stronger security: authentication, confidentiality, authorization and integrity.

The purpose of this White Paper is to review the market requirements in terms of security, to define what a Smart USB Token is and to demonstrate its benefits.

2. Market Environment

In today’s environment, the need for organizations to increase connectivity and facilitate access to their networks is growing dramatically, what raises questions about securing the user access.

Banking sector:

Banks recognise the importance of the strong authentication for their online customers. Online Banks are losing 30 million customers a year as they fear phishing attacks, fraudulent transactions and ID theft. Fraud is clearly putting online banking at risk of collapse.

Governments:

The growing usage of Government portals like tax or custom declaration, access to information or transactions raises questions about privacy, security and convenience. The need for ID management will inevitably increase as online services will become more and more popular.

Enterprises:

Securing the access to the network is becoming a key issue for Enterprises. Although passwords still represent the majority of current security access tools, their weaknesses raise questions to Enterprises: how to authenticate network use access while keeping operations up and running?

Mobile Operators:

With the rapid deployment of the wireless technologies (like WiFi), new services offered by internet access providers (like VoIP) could rapidly become a major threat for Mobile Operators. In order to offer new services for their subscribers, Mobile Operators are looking for portable and personalized devices which can securely support their new applications.

3. Smart USB Token Definition

In our definition, a Smart USB Token:

- Contains a tamper-proof micro-controller and software for authentication and secure storage
- Supports personalization by the issuer
- Is portable and USB connected

Some OTP Tokens which do not contain any secure hardware and software do not belong to our definition of Smart USB Token.
From the point of view of functionalities, the Smart USB Token stores the data such as the user's credentials, digital certificates, and private keys, or stores the client application programs that are used to generate a dynamic password or a credential valid for a specific network session. When the device is plugged into the USB port of the computer, the user is prompted to input his or her PIN, which acts as the second factor of authentication.

Hardware authentication devices serve as users' digital identity organizer, managing their varied credentials whether they are encryption keys or passwords, on one device. This eliminates the need to remember several different passwords to access different databases in the network. Users simply plug the device into a standard USB port on the PC and enter their PIN for PC security and remote access. Users are expected to embrace the security solution due to its ease-of-use and the real-time remote access to what they need exactly when they require it.

4. Benefits for the Industry

Smart USB Tokens and smart cards are identical in many respects in terms of security and technology. Smart cards and Smart USB Tokens with built-in cryptographic processors are viewed as the most secure vehicle for implementing digital signatures in a PKI.

Both have embedded secured integrated circuits and memory to enable them to store and process digital data. They differ mainly in their form factor and the interface used by them to connect to the network or the user device. Smart USB Tokens are by construction more convenient for the end users as they offer an easy access to plenty applications through their computer. Furthermore, the Smart USB Token matches the current set up for Smart Card manufacturing; similar manufacturing process can be used for higher value applications. Smart USB Tokens can be positioned as an innovative solution in the Smart Security world.

5. Market requirements by applications

Defining Market requirements is complex for 2 reasons. Firstly, the market is just emerging, so it is not enough mature to identify all needs. Secondly, for the same kind of applications, requirements are not the same, depending on the country, the enterprise, etc.

However, a solution based on the Smart USB Token is a global solution containing:

- Hardware (tamper proof micro-controller)
- Applet in the secure element
- Middleware in the flash memory eventually
- Server

Normally defined requirements should concern all parts of the solution. In this White Paper, we will extrapolate only the specificity of the Smart USB Token from the current smart card market:

- The Smart USB Token must be certified according to ROHS and CE standards (specific USB Token);
- For some high end applications, the security implementation should be certified (e.g. according to common criteria level EAL 4 or 5, FIPS or other relevant schemes) or type approved as often practised in the banking world;
- The communication between the Secure USB Token and the server must be secure (PKI for government, EMV for payment, etc);
- The Smart USB Token should support the requirements for digital signatures, in particular with respect to the upcoming CEN standard EN14890-SmartCards as secure signature devices;
- For Governments, the solution should be standardised; for example, current investigation to define interoperable health card (European implementation);
- The data stored in the Smart USB Token could be replicated on the server side;
- The Smart USB Token will need personalization to implement unique user identification;
- The price of the Smart USB Token should be competitive against former solution;
- Today, to run a Smart USB Token without further installation requires either Driver, Middleware or Administrative right. While in enterprise environment, middleware/driver base solutions might become the right answer, for the general user a solution that does not require administrative rights or middleware/driver is a problem left to be solved. Microsoft’s Universal Plug'n Play would be the answer (figuring the Smart USB Token as Network Card) but UPnP is still under development and does not yet satisfy the demand.

6. Use cases

Government to Enterprises

Government portals are increasingly offering or requiring a user ID for Enterprises to access parts of the public sector Web presence. The chronology starts with publishing information to Enterprises, then moves to interaction, delivering and receiving information from Enterprises, then moves to transaction, undertaking some government processes online. Information and communication technologies provide tremendous leverage in accessing, processing, manipulating and stealing information. This raises questions on privacy, security and fair information practices on one hand, to be balanced on the other hand against convenience of e-Government service delivery that is capable to identify and apprehend terrorists and fraud artists.

The need for some form of identity management will increase for Enterprises as Governments continue to integrate information systems for online service delivery. The challenges are to identify, authenticate and authorize the service per sign-on function per each login session. Besides, the ability in creating, using, changing and ending a user associated with multiple identities is crucial, as it involves technical, procedural, legal and policy dimensions.

For example, tax services that apply to Enterprises were made available in most countries through government portals. The end user will first proceed to the registration process with a validate identification such as Enterprise registration in order to obtain online identification, password and tax declaration credential. The end user can then declare tax, update Company details or even make tax payments with the unique user credential. The level of security and user assurance increases as the level of service involves personal information and transaction. Since it will impact end user's trust in the online government services as well as fraud settlement, the strength of Smart USB Token is to make trust, ease of use and convenience possible. The Smart USB Token ensures indeed legitimate use via strong authentication, something you have and something you know (Personal Identification Number PIN), ease of use with USB connectivity to any PC, and finally convenience because of portability of trusted personal ID which can be used between different computers.

Strong authentication and authorization of e-Government administrative services are getting more popular. We see several types of e-Government services available for Enterprises such as tax declaration, custom declaration, etc.

Enterprises

The cascading effects of pervasive network access and an ever-increasing amount of digital information present Enterprises with a new array of challenges. Information loss is costly, whether it is due to theft or accident, and it can adversely impact an enterprise's reputation and financial performance. According to a study done by Ponemon Institute in 2006, data breaches cost companies an average of $182 per compromised record, a 31 % increase over 2005. The Computer Science Institute estimated an average theft of a laptop cost a company $89,000 due to lost of confidential information. In addition, regulations such as Sarbanes-Oxley, European Union Data Protection Directive, and the Health Insurance Portability and Accountability Act (HIPAA) are forcing enterprises to invest in new infrastructure and technologies to meet the requirements for enhance protection of their networks, applications and data.

The challenges are to balance the defence of organization's computer systems while keeping operations up and running to support business activities. In addition, many countries have national policies for protecting customers or confidential data. All these factors shall be considered when taking decisions about managing security. Thus, the outcome will take into account information security, data security, regional risk, and physical security in one big picture.

IDC defines the Personal Portable Security Device (PPSD) Market as the following: an Evolving Component of the Authentication and Authorization Ecosystem in one of the Industry Developments and Models report. It said, "IDC believes the external security device market is experiencing both convergence and evolution, especially as related to multifactor authentication and end-to-end digital identity products and services." External security device is instrumental in managing security because of its convenience, portability and security implementation.

For example, remote Web access services for employees and business partners, the business exchange such as email, document, ordering status, and transaction bring efficiency in business and increase services. However, sensitive information leakage may cause Enterprises a fortune due to reputation and legal settlement. The use of username and password belongs to the past as it is weak and has significant impact on Enterprise's hotline support. Increased security can be implemented and simplified with the use of Smart USB Token, with its strong authentication of user, which eliminates the weak username and password, and the user credentials can also secure information exchange over the Internet.

Banking

Consulting and managing one's bank accounts from home or any other place when travelling has already proven to be very convenient for users. This is also convenient for banks which can then afford to have their employees in local offices focusing on added value services rather than basic daily banking operations.

However such online services raise the issue of the security level. For only consulting bank accounts, confidentiality and privacy are the main issues. For moving money from one bank account to another one, which can be at a different bank in some cases, the risk of theft has become critical.
For example, *phishing* is a method of fraud through internet, consisting of acquiring personal customer data such as name, bank account number, access password, that is to say *thief their identity*, in order to access their bank account and steal their money. It has been established that two thirds of banks have been the target of *phishing*, and Online Banks lose 31 million customers a year because of security concerns.

In this context of increasing cyber fraud, static passwords are no longer secure enough and more secure methods are necessary to meet all together the four security requirements: user authentication, data integrity, transaction confidentiality and non-repudiation.

In this environment, the Smart USB Token is the ideal solution, already adopted in certain countries : the state of the art security provided by the secure MCU and its associated software, combined with the USB connection to the PC, will enable to meet the above mentioned four requirements : strong user *authentication* thanks to unique identification of each personalized device, *data integrity* and *confidentiality* thanks to encrypted communications between the PC and the distant server of the bank, and *non-repudiation* of the transaction thanks to the digital signature. In addition, the Smart USB Token will securely store all the necessary encryption keys to ensure the best available security level, certified by independent Authorities.

Mobile Operators

With the deployment of wireless technologies (WiFi, WiMax), travellers can now easily download specific software like "Skipe" to make phone calls through their personal computer rather than using their mobile phone. This method could be seen as a major threat by Mobile Operators who are getting substantial revenues from the "roaming" services. In order to reply to this threat, some Mobile Operators are proposing Smart USB Token allowing the subscriber to connect to internet through his/her computer and to use VoIP features to make phone calls in a more cost effective and convenient way.

Other business cases

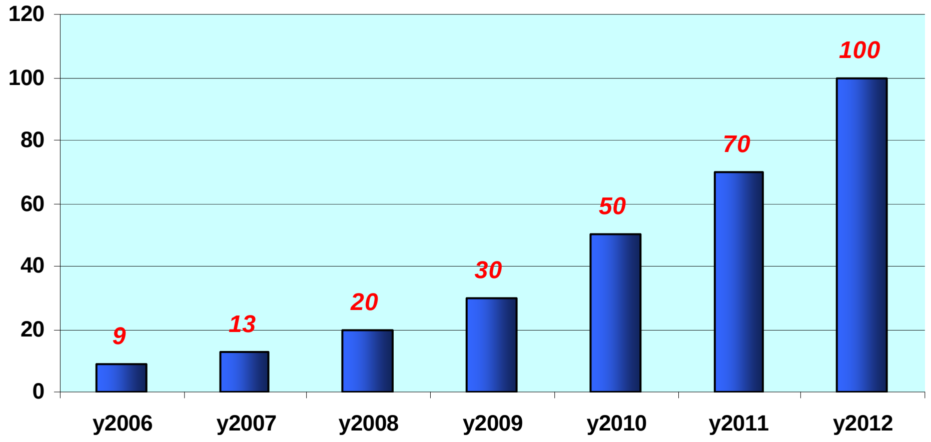
There are certainly several other business cases for Smart USB Token. Among those cases, Education must be mentioned, as there is a case for student to carry Smart USB Token for Secure access and for Secure storage.

7. Conclusion

Passwords are not enough: the need for more secure authentication is definitively growing. Smart USB Tokens are the most convenient personalized, portable and USB connected devices which feature secure hardware and software for robust authentication and secure storage. They combine the encryption capabilities of a smart card with the versatility of the Token.

In this context, it is not a surprise to note that Smart USB Tokens are entering the steady growth stage with an expected 30% annual growth rate.

Smart USB Token Market Evolution-Millions units per year (source Eurosmart)



EUROSMART
The Voice of the Smart Security Industry

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