A Trusted Smart Phone and Its Applications in Electronic Payment

Changying Zhou

A Trusted Smart Phone and Its Applications in Electronic Payment

Changying Zhou

Chunru Zhang

Special Note: this paper was approved using our English as a second language editorial procedures. We feel the content is timely and important. Stephen Northcutt

Abstract

With the growing intelligence and popularity of mobile phones and the trend of cellular network's convergence to IP based network, more and more mobile applications emerge on the market. This paper analyzes the building blocks of the trusted smart phone and proposes a framework to provide a trusted platform for mobile electronic payment.

1. Introduction

With the explosive growth of the mobile phone usage, increasing computing power of cell phone, and the convergence of the cellular network to IP based network, e-Commerce is further extending its tentacles to the mobile network. Many service providers of cellular networks are offering the convenience of paying bills with mobile phones. Hence, there is a growing demand to make the mobile phone more trustworthy. Identity theft, virus, spyware and other malicious code in the computer world emphasize the need for a trusted mobile phone.

With the Trusted Platform Module (TPM) technology [6], the Trusted Computing Group (TCG) offers a potential solution for the trust on e-Commerce including mobile phones. TPM provides root of trust, which is a secure chip consisting of cryptographic engine and protected storage. However, the mobile phone with TPM embedded is not equivalent to a trusted mobile phone. As [1] demonstrated, the Operating System (OS) of smart phones should also implement a reference monitor concept: mediate all accesses, be protected from tampering, and be verified as correct. Specifically, there is a requirement for trusted input/output subsystems. Built upon the TPM and trusted OS, a trusted phone should include identity system supporting services for diverse applications such as electronic payment. The identity metasystem serves as a standard interface to different identification and authentication (I&A) mechanisms such as password, Kerberos, digital signature and biometric. Microsoft InfoCard is an example of identity metasystem

implementation [3]. By piecing these systems together, we can create a mobile payment framework and mobile payment applications.

2. The potential of smart phone

In comparison with other platforms upon which electronic payment is based, such as the PC and smart card, the proposed smart phone has many advantages, which might make it possible to become universal electronic payment vehicle in the future.

The PC, lack of hardware based protection measures, is not a secure platform to conduct electronic payment. The rampant identity theft and spreading of virus and other malicious codes highlight the weakness of the PC in security. Although the recent trusted computing initiative from Trusted Computing Group aims in part to address the security issues through both hardware and software based approaches, the open system nature of the PC, which can install and run arbitrary software, makes it difficult to be trustworthy [1]. However, the smart phone can be designed to be more secure: embedded TPM to secure chip and storage, tamper-proof mechanisms to secure the input and output, securely crafted OS to insulate itself from tampering and bypassing by applications running above. This may be easily achieved due to the fact that the smart phone is not an open system. The OS, especially the device drivers, cannot be modified by end users, and applications cannot be arbitrarily installed by end users. Moreover, the smart phone has the merit of mobility over the PC, and even the laptop is awkward to carry comparing with a handset.

The smart card has the advantages of ease of use, easy to carry, and security, which are shared by the smart phone. However, the smart card doesn't provide trusted input and output, and it has to interface with smart card reader that is further connected to a PC. As explained before, such a PC may not be trustable, and a compromised PC may allow a virus or Trojan horse to intercept the input/output flows: if the transaction requires the user to key in some sensitive data, it is at risk of being intercepted; the data shown in the computer monitor may not be the same as the data transmitted to the smart card, etc. In contrast, the Input/Output subsystem of the smart phone can be made trustworthy by tamper proof or tamper resistant mechanisms.

3. Building blocks of the trusted smart phone

Now that we have shown the potential of a smart phone to be fortified to enable secure online payment, and explained its advantages over other platforms, we will further examine the security requirements of a trusted smart phone.

3.1 Trusted Platform Module (TPM)

The root of trust lies in the Trusted Platform Module [6]. The TPM is basically a secure microchip with added cryptographic capabilities and hardware protected storage. A set of cryptographic functions are executed within the TPM hardware:

- RSA accelerator, which is used during digital signing and key wrapping;
- Hash algorithm engine, specifically SHA-1 engine, which is used to compute hash values of small pieces of data (large pieces of data are hashed outside of the TPM for better performance);
- Random number generator for key generation.

Hardware and software outside of the TPM have no direct access to the execution of these crypto functions within the TPM, except for the invocation of the services provided by the TPM through its well defined interfaces.

Strengthened by the TPM, the smart phone is capable of integrity measurement, storage and reporting, which creates the hardware based foundation for trust. The integrity measurement is aimed at key platform characteristics that affect the integrity and trustworthiness of a platform, such as OS loader, OS and device drivers, etc. These integrity metrics obtained in integrity measurement are kept in hardware protected storage for future attestation that establishes the trust.

Specifically, trust of the smart phone is established through a chain of integrity measurements and execution transitions: during boot-up, the TPM measures the OS loader; after TPM attests that OS loader is trusted, the execution is transferred to the OS loader; the OS loader and TPM then measure the OS, including the device drivers; after the OS is attested as trusted, the execution is transferred to the OS. The OS can further attest applications running above it.

3.2 Trusted OS

The simple addition of TPM to the smart phone doesn't result in a trusted smart phone. Its OS should implement the reference monitor concept [1].

The smart phone OS should not be bypassed. It mediates every access to system resources and data, determining whether the requested access would lead to compromise of security. The smart phone OS may take advantage of the CPU which implements the Multics Ring Architecture: only the OS is capable of running within ring 0 (the most privileged), and any application is only allowed to run within the unprivileged rings, which have no direct access to memory, input and output subsystem, and other system resources without the mediation of the OS.

The smart phone OS should be protected against tampering to ensure that attackers cannot subvert the enforcement of security policy. Especially, it requires that the running applications should not tamper the OS. The ring based architecture of CPU and memory segmentation of Memory Management Unit (MMU) combined together are able to enforce effective domain separation and confinement. Moreover, to avoid physical attack, the smart phone may employ tamper-proof or tamper resistant physical security mechanisms.

The smart phone OS should be made small enough to validate its integrity. Fortunately, unlike the OS running on PC, i.e. a general purposed operating system, the smart phone OS can be scaled down to a least common denominator, affordable to be analyzed, evaluated and tested for its integrity.

The OS and device drivers shall not be dynamically loadable. This avoids the pitfalls of the PC: the generally purposed operating system demands much more sophisticated ways to meet the requirements of non-bypassing and tamper-proof, and therefore makes the kernel code swell explosively. The usage of the mobile phone justifies this requirement, because the end user seldom needs to re-configure the OS and device drivers. Meanwhile, installation of applications will fail if it does not pass the verification of digital signature or checksum.

3.3 Identity Metasystem

Another merit of smart phone is its versatility in supporting a variety of identification and authentication mechanisms. It can support password, Kerberos, LDAP, and digital signature with the support of underlying TPM and hardened OS. It can even employ biometric mechanisms (such as voice, iris, retina, fingerprint etc.) by modifying its microphone system, screen or embedded camera to be multi-purposed.

Realizing the potential of smart phone in identification and authentication application, it would be natural to turn smart phone into a component of an identity metasystem [3]. For example, it may play an active role in the Microsoft promoted "InforCard". Connected to the computer via BlueTooth or USB, it may serve as an abstract layer of interfaces to diverse identity systems, providing interoperability among them, and enabling creation of a consistent and common user interface. Especially, its physical protection mechanisms against tampering and spoofing may be leveraged in the identity metasystem.

3.4 Other Ways to Enhance Security

Except for the requirement of implementing the reference monitor concept, there is another requirement of making the smart phone trustworthy, i.e., providing trusted path for user input and output. The tamper-proof or tamper resistant mechanisms may be

implemented in the smart phone to protect against physically installing a bug in-between the keypad/screen and the secure chips in order to divulge sensitive information or tamper with the input/output data flow.

Because of its size and mobility, the smart phone is vulnerable to theft. As a countermeasure, the smart phone can be strengthened by the inclusion of self-destruction mechanism. When the smart phone is stolen, the owner may contact the service provider to invoke the self-destruction mechanism, which makes the handset useless to the thieves. The anti-theft feature may be further facilitated by adding a global positioning system (GPS). Now it is possible that the cell phone tower can pinpoint the cell phone's location.

4 Electronic Payment Systems

Roughly speaking, Electronic Payment Systems are those network services, such as the services over Internet, which involve exchange of money for physical goods like books, or electronic goods like music and video clips. A generic electronic payment system is illustrated in Figure 1.

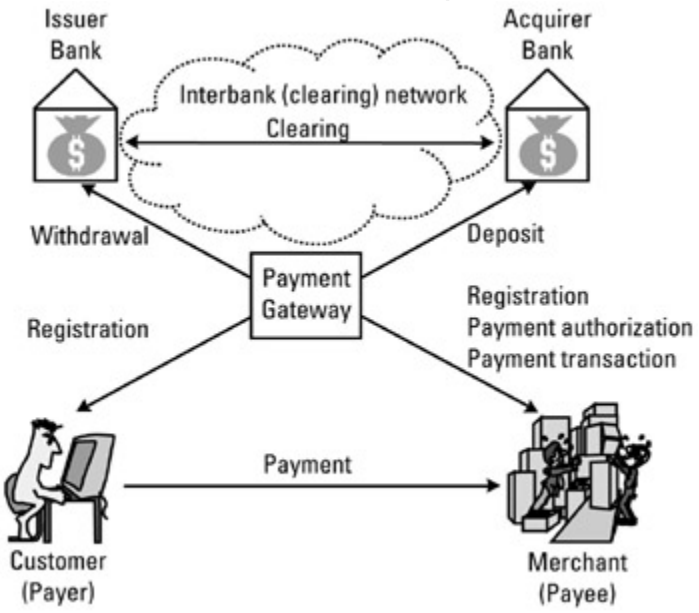

Figure 1: A Generic Electronic Payment System

A customer and a merchant should register with the payment service provider to participate in the electronic payment system. The payment gateway, run by the payment service provider, connects the public network to inter-bank clearing network, so that the customer is associated with its bank (referred to as issuer bank) and the merchant is associated with its bank (referred to as acquirer bank). When the customer purchases goods or services, he/she sends the payment instruction to the issuer bank and order information to the merchant. The merchant requests the payment gateway to authorize the payment. If the authorization goes successfully, the payment gateway finalizes

transaction over the inter-bank clearing network by informing the issuer bank to withdraw the specified amount of money from the customer's account and deposit it to the merchant's account at the acquirer bank. The gateway then acknowledges the merchant so that the latter can arrange the delivery of the goods or services to the customer.

The payment instruction (PI) may be sent from the customer to the merchant, and the merchant further relays it to the payment gateway; or the PI may be sent from the customer to the payment gateway directly. The transmission of PI may employ the following open network channels, to name a few:

- A TCP/IP channel (wired or wireless) over the Internet;
- A WAP channel over the cellular network;
- A SMS channel.

Since the advent of the Internet, several electronic payment systems have been proposed and put into service, such as the dedicated account-based systems such as PayPal, ISP involved payment systems, credit card based systems, debit card based systems, electronic cash systems and micro-payment systems etc. Before we draw a whole picture of the mobile payment framework with the support of the trusted smart phone, let's first take a look at different electronic payment systems.

4.1 PayPal

PayPal [4] is an online payment service, provided by e-Bay, which allows individuals and business to transfer funds electronically. It requires the seller and buyer to have PayPal accounts and provide their bank account or credit account information that is associated with their PayPal accounts. Both the buyer and the seller deal with PayPal. PayPal, in turn, handles all transactions, deals with various banks and credit card companies, and pays the interchange charge. PayPal uses SSL/TLS to protect payment information in transit and heavily relies on user passwords for payment authentication. Hence it is exposed to vulnerabilities such as weak password, phishing attack, spoofing and email scam.

4.2 ISP Involved Payment System

The distribution of some kind of electronic products over communication networks (such as video-on-demand) leads to a payment system which involves ISP [2]. Because the telecommunication network connects the consumer and content provider to the ISP, the ISP may act as an independent service provider for payment services. The ISP may identify the subscriber's identity and bill information, and then charge transactions to the subscriber's account held at the ISP. However, such payment systems are only applicable to limited electronic goods or services, therefore its application may not be widespread.

4.3 Credit Card

Credit card based electronic payment is currently most popular in the Internet. It is similar to the traditional use of credit cards, except that it doesn't require the cardholder's signature: the customer sends his/her credit card information (i.e. credit card number, expiry date, etc.) to the merchant. The merchant requests the acquirer bank for authorization. The acquirer bank communicates with the issuer bank over the inter-bank clearing network, asking for authorization. The issuer bank acknowledges the authorization request, and the acquirer bank notifies the merchant of the result. If successful, the merchant may deliver the goods or services to the customer. The issuer bank then sends the bill to the customer which pays the charges to the bank by other means (for example, check, bank transfer, etc.). From the description of the generic credit card payment process, it is obvious that such a payment system is vulnerable to the disclosure of credit card number. Once disclosed, the credit number can allow anyone to pay with the owner's credit card. This situation becomes more serious when the online credit card payment can potentially make large-scale fraud.

Various security measures have been taken to protect online credit card payments. SSL/TLS secures the communication channel between the customer and the merchant, preventing the payment information from being disclosed to eavesdroppers. This is the most popular way to make online payment secure. However, it still doesn't prevent the dishonest merchant from misusing the payment information. More importantly, there is no end-to-end trust relationship between the customer and the merchant, and it doesn't provide the non-repudiation of payment and delivery.

To strengthen the security of online credit card payments, Visa, MasterCard and other participants proposed a secure payment protocol called Secure Electronic Transactions (SET) [5]. The SET makes use of various cryptographic mechanisms to secure the electronic transaction. Particularly, public key cryptographic system plays a key role, and PKI is incorporated into SET to establish certificate authority (CA) hierarchy upon which the trust relationship relies. CA signs the cardholder certificate, merchant certificate and payment gateway certificate to vouch the authenticity. The payment process consists of the following main steps:

- Payment Request – The customer prepares the payment instruction (PI), including credit card number and other private information, and encrypts it to make sure it is only readable to the Payment Gateway. The customer also prepares order information (OI) and encrypts it so that OI is only readable to the Merchant. Finally, it generates a dual digital signature of PI and OI (similar to the traditional signature), by which the customer can bind the PI and OI together and authorize the transaction. The customer sends all of the information to the merchant.
- Authorization – After receiving Payment Request, the merchant retrieves the OI and prepares the authorization request message. It packages the authorization request, PI (received from the customer), dual digital signature of PI and OI (received from the customer), and the hash of the OI without exposing the content

of OI, which is used for the Payment Gateway to verify the dual digital signature of PI and OI. The merchant sends all of them to the Payment Gateway. After receiving the authorization request, the Payment Gateway extracts the PI, dual digital signature of PI and OI, and other information. It then verifies the dual signature of PI and OI, and makes an authorization request to the acquirer bank, which, upon receiving the request, follows the traditional way to settle the transaction (it is out of the scope of SET).

- Capture – The merchant requests the final settlement of the payment after successful authorization, which involves transferring of money from customer's account at issuer bank to merchant's account at acquirer bank.

The SET provides enhanced security: it no only provides non-reputable services, but more importantly keeps the customer's private information (such as credit card number) from merchant's access.

4.4 Debit Card

The debit card offers direct access to the customer's bank account in point-of-sale (POS) transactions. The merchant is equipped with POS terminal. The customer interacts with the PIN PAD by swiping the debit card and entering the PIN on the PIN PAD to make the payment. The PIN PAD and POS terminal are physically secured by tamper proof or tamper resistance mechanisms, and the PIN is encrypted before transmitted to the issuer's bank server.

However, there is a concern for the debit card use over public communication channels with a PC: due to the lack of proper security and authentication, as explained in Section 1.1, banks consider the consumer's PC as an insecure device, compared with the POS terminal and PIN PAD at the physical store. In this scenario, the proposed trusted smart phone demonstrates its particular advantage as it can be directly participated in debit card payments, or indirectly adapted to be an intermediary device for reading the debit card.

4.5 Electronic Money

Electronic money, or digital money, is the electronic representation of traditional money [7]. Most electronic money systems employ blind digital signature technology in order to make the payment anonymous and secure on the Internet. The customer "mints" the digital money. His/her bank signs the issued digital money and subtracts the amount from the customer's bank account. The customer then stores the digital money in an e-wallet. Whenever the customer makes purchase, he/she transfers the digital money from the e-wallet to the merchant, who further forwards it to the bank. The bank will then verify the validity of the electronic money, check against double-spending, complete inter-bank clearing, and exchange digital money from different banks. The electronic money is finally deposited into the merchant's account.

The electronic money systems not only take advantage of blind signature technology to implement anonymity and authenticity, but also use trusted e-wallet to safeguard against forging, stealing of digital money and double-spending. As described before, the proposed trusted smart phone may be an ideal choice for this kind of e-wallet.

4.6 Micro-payment

Micro-payment is designed to handle low and micro value payments. In a micro-payment system, small charges are aggregated before they are settled with the payment systems to achieve cost-efficiency by cutting down the overhead involving in the payment [2].

The micro-payment system may take the form of centralized account management, electronic tokens, etc. The centralized account management system processes the transfer orders among accounts. The micro-payment accounts may be loaded in advance or charged afterwards. The electronic tokens simulate the physical coins. The exchange of such tokens realizes the payment function. The user needs to "buy" electronic tokens first, in a way as described in the electronic money section. The vendor collects the electronic tokens over time and exchanges them for real cash.

Either way, the proposed trusted smart phone may provide necessary cryptographic functions and secure storage capability to support Micro-payment.

4.7 IOTP

The Internet Open Trading Protocol (IOTP) is not a separate payment system [7]. Indeed, it is a common electronic payment framework in attempt to ensure interoperability among different payment systems. This means that any electronic payment system can be used within the framework. The specific parts of the protocol of the underlying payment system are contained in a set of payment scheme that supplements the IOTP specification.

5. A Mobile Electronic Payment Framework

After we presented the security measures applied to fortify a smart phone, and introduced variant electronic payment systems, now we will put the pieces together and propose a mobile electronic payment framework, as illustrated in Figure 2.

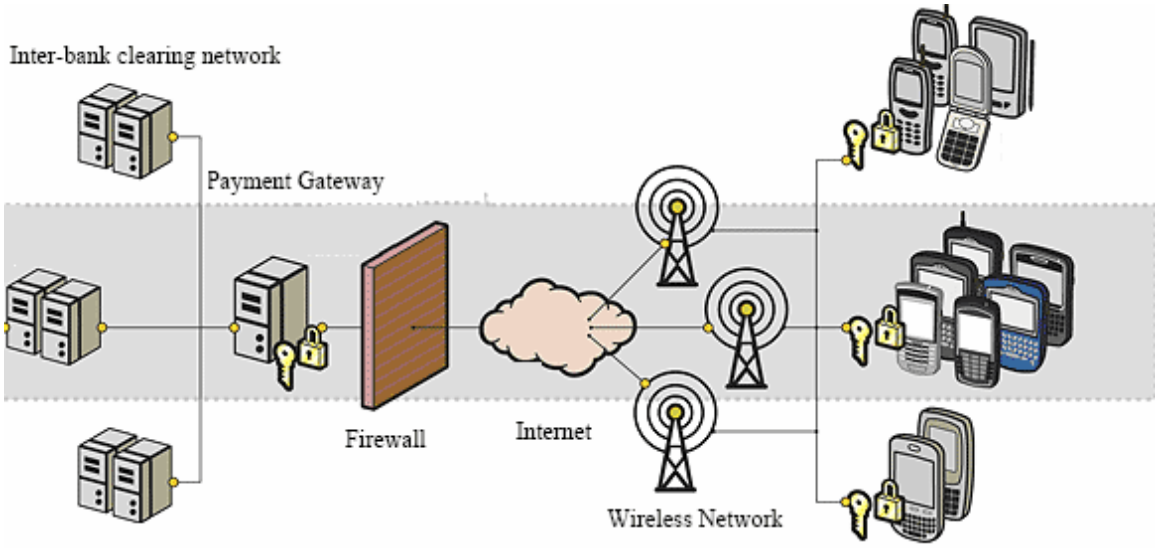

Figure 2. A Mobile Electronic Payment Framework

Following the generic electronic payment system, in such a mobile electronic payment framework, the participants of mobile payment involves the customer, merchant, payment gateway, issuer bank, and acquirer bank.

The customer is equipped with a secure smart phone. Such a secure smart phone serves as e-wallet, and the mobile payment application is loaded into the smart phone as a trusted application: before running the application, the OS verifies the integrity and trustworthiness of the mobile payment application with the aid of TPM; only when the verification succeeds, may the mobile payment application be invoked. The runtime security of the mobile payment application is further enforced by the OS, which implements the reference monitor concept.

The secure smart phone may choose one of the following payment channels:

- TCP/IP channel over the Internet;
- A WAP channel over cellular network, such as GSM network;
- Short range radio channel (such as Bluetooth technology), connected to POS terminal or vending machine.

There is a special security problem with gateways in the situation of mobile payment over the cellular network. The WAP- or IP-gateway in the GSM and GPRS/UMTS network respectively connects the Internet to the mobile operator's internal network and finally the air "interface". If the protection of payment information is reliant on the transport security, payment information that is securely sent over the mobile network is decrypted

in these gateways before it is encrypted and securely sent over the public Internet to the relevant financial institution. Therefore, unauthorised persons may be able to obtain sensitive transaction information from the gateway. It is hard for financial institutions to supervise these gateway systems. Hence, we encourage the security measures at application level (such as SET), instead of transport level (such as SSL/TLS, or WAP transport security protocol).

The merchant may choose to have its own web site with online payment feature, or be equipped with POS terminals or vending machines (like the ones installed in gas station). Big retailers may take advantage of RFID technology to facilitate the electronic payment.

The mobile payment framework may follow the IOTP and support variant electronic payment systems: such as credit card, debit card, digital money, micro-payment, etc. The following are three use case scenarios of the mobile payment framework.

5.1 Credit Card

The customer surfs the Internet with his/her smart phone. He/She finds books he/she is interested in and puts them in the shopping cart. Finally, he/she clicks the pay button to invoke the payment process, which launches the underlying credit card mobile electronic payment system. The mobile payment application retrieves the credit card information in the e-wallet, applies the private key to digitally sign the payment instruction, pull the merchant and payment gateway public key certificate to encrypt order information and payment instruction. After finishing preparation of the payment request message, the mobile payment application sends it out to the merchant. The merchant verifies the payment request, and forwards the payment instruction to payment gateway for payment authorization. Payment gateway validates the request of the authorization, and knowledge the merchant of the result. The merchant sends the receipt to the customer if successful; otherwise, rejects the transaction. The customer may wait for the delivery of the books.

5.2 Debit Card

The scheme in Section 5.1 is also applicable to debit card electronic payment system by replacing credit card number with bank account information. Here, another example is illustrated as below.

The customer goes shopping at a supermarket. He/she uses his/her smart phone to retrieve the product information of the merchandise of his/her interests (for example, via communicating with the RFID tag on the merchandise). Before he/she takes the goods out of the supermarket, he/she invokes the mobile payment application in his/her smart phone to make the payment: the smart phone contacts the POS terminal remotely (for example, via Bluetooth like short range radio technology), prepares the payment instruction based on the product information stored in the smart phone and account information stored in the e-wallet, encrypt and digitally signs the payment information,

and sends it to the POS terminal. The POS terminal forwards the payment information to the bank server which settles the payment.

5.3 Digital Money

The customer fills its e-wallet in the smart phone with digital coins beforehand. When he/she tries to park his/her car at a metered parking lot, he/she points his/her smart phone at the electronic meter, retrieves the rating list, makes choice of the time he/she intends to park his/her car, and clicks the key to pay. Behind the scene, the digital coins are taken from the e-wallet, and "deposits" into the electronic meter. Now the meter shows that he/she may be allowed to park his/her car for specified time.

6. Conclusion

The proliferation of the mobile communication and trend of mobile network's convergence to the IP network, inspire growing demands of mobile applications. Security and trust are among those enabling factors for the mobile applications (even for web services) to take off.

The paper outlines the security measures which are applied to smart phone to make it trustworthy. The secure smart phone acts as an e-wallet and serves as a key component for the electronic payment systems. In addition, it can also play an important role in identity metasystem.

The paper also briefly examines variant electronic payment systems. Furthermore, it proposes a mobile payment framework, in which the secure smart phone acts as an e-wallet. Finally, it demonstrates several use case scenarios of the mobile payment framework.

Reference

[1] Jason F. Reid, William J. Caelli: DRM, Trusted Computing and Operation System Architecture, In *Australasian Information Security Workshop 2005*, Newcastle, Australia.
[2] GigaABP: Electronic Payment Put in Context, 4 March 2002
[3] Microsoft: Microsoft's Vision for an Identity Metasystem, May 2005
[4] PayPal: How PayPal Works, In *http://www.paypal.com*
[5] SETco: SET Secure Electronic Transaction Specification, May 1997
[6] TCG: TCG Specification Architecture Overview, Revision 2.1, 28 April 2004
[7] Vesna Hassler: Security Fundamentals for E-commerce, Artech House, 2001