SOPAS: A LOW-COST AND SECURE SOLUTION FOR E-COMMERCE

Marc PASQUET[1], Delphine VACQUEZ[2], Christophe ROSENBERGER[1]
[1] Laboratoire GREYC: ENSICAEN – Université de CAEN – CNRS
[2] DRI (Department of Industrial Relationships): ENSICAEN
6 boulevard Maréchal Juin, F-14020 CAEN (France).
marc.pasquet@ensicaen.fr
delphine.vacquez@ensicaen.fr
christophe.rosenberger@ensicaen.fr

KEYWORDS
Smartcards, Authentication, Security for E-Business, Commercial and Industry Security.

ABSTRACT

We present in this paper a new architecture for remote banking and e-commerce applications. The proposed solution is designed to be low cost and provides some good guarantees of security for a client and his bank issuer. Indeed, the main problem for an issuer is to identify and authenticate one client (a cardholder) using his personal computer through the web when this client wants to access to remote banking services or when he wants to pay on a e-commerce site equipped with 3D-secure payment solution. The proposed solution described in this paper is MasterCard Chip Authentication Program compliant and was experimented in the project called SOPAS. The main contribution of this system consists in the use of a smartcard with a I^2C bus that pilots a terminal only equipped with a screen and a keyboard. During the use of services, the user types his PIN code on the keyboard and all the security part of the transaction is performed by the chip of the smartcard. None information of security stays on the personal computer and a dynamic token created by the card is sent to the bank and verified by the front end. We present first the defined methodology and we analyze the main security aspects of the proposed solution.

INTRODUCTION

E-commerce is one of the most challenging issue in computer science nowadays. Many e-payment architectures have been proposed in the last decade (Kleist, 2004; Konar, & Mazumdar, 2006; Ekelhart et al., 2007). Nethertheless, very few have been used in real conditions for e-commerce. One major reason is that the defined solution must be supported by major card schemes such as Mastercard or/and Visa. In the following, we present two solutions that were defined within this context.

To limit the risk that the customer can repudiate his payment transaction, a set of companies (Visa, MasterCard, GTE, IBM, Microsoft, Netscape, SAIC, Terisa system, Verisign) have developed, in the eighties one solution call SET (Secure Electronic Transaction). The customer's bank sends him one certificate issued from one CA (Certification authority) of a PKI (Public Key Infrastructure) which is stored on his computer. When he wants to realize a payment on the Web, the customer must sign with the PKI keys (Rennhard et al., 2004).

Another solution for electronic payments is 3D secure (3D–Secure Functional Specification, 2001) developed by VISA and used by MASTERCARD. The commercial trademarks are « Secure Code » for MasterCard and « Verified by Visa » for Visa. The term 3D is the contraction of "Three Domains":

- Acquiring domain (acquiring bank and merchant) ;
- Issuer domain including the customer authentication;
- Interbank field which makes it possible the two other fields to communicate on Internet.

The client realizes his purchase on a merchant's Website that is 3D-secure compliant and click on the payment icon ("MasterCard SecureCode" or "Verified by VISA"). He is invited to enter his card scheme, card number and expiration date. The MPI (Merchant Plug-In) installed in the merchant's website, contacts the Visa or MCI directory to obtain the Internet address of the issuer. Then, using the client's personal computer, the MPI contacts the issuer with a formal PAReq (Payer Authentication Request) message. The client's authentication is under the bank responsibility. When that last task is realized, the bank issuer answers to the MPI of the merchant's website with a formal PARes (Payer Authentication Response) message. The MPI sends an authorization request to the acquiring bank which transmits it to the issuer which will answer with an authorization number. This last dialog is realized to be completely EMV compliant (Europay MasterCard and Visa). The internationally agreed standards for chip payment cards. EMV standards are maintained by EMVCo (EMVCO, 2000). In fact, with 3D-secure, the authentication problem from the customer / merchant domain is replaced by the customer / issuing bank domain (see Figure 1).

Proceedings of the 2008 High Performance
Computing & Simulation Conference ©ECMS
Waleed W. Smari (Ed.)
ISBN: 978-0-9553018-7-2 / ISBN: 978-0-9553018-6-5 (CD)

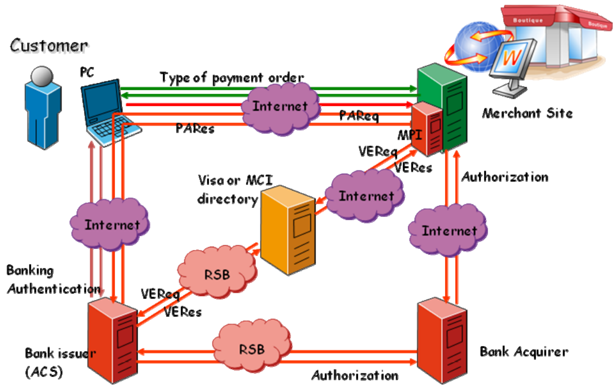

Figure 1: The different communications in 3D-secure payment

The most important challenge today in the 3D-secure architecture for a bank issuer, is to authenticate one client with as many guarantees as possible with the lowest cost. The goal of the SOPAS project in which we are involved in, is to propose new e-transaction architecture. The objective is then to develop a secure and a low-cost solution that can be attractive for banks considering security and commercial issues. We show in this paper some elements on the security of the proposed architecture and the reasons why we think this solution can be supported by major card schemes.

We describe in the next section, the proposed architecture defined within the SOPAS project. In the third section, we focus on the security issues of the proposed solution. Conclusions and perspectives of this work are given in the lat section.

SOPAS PROJECT

The idea of the SOPAS project is to fulfill two services for one client. The first one is the payment on an e-commerce site equipped with a 3D-secure payment solution. The second service deals with remote banking and concerns the use of a personal computer by a client through the web to access to his bank account and to realize different operations (consultation or bank transfers for example). We think that the proposed solution must allow this last service for economical reasons. A bank could be ready to adopt the solution even it will cost some more money if it can offer an additional service for a client. Remote banking is generally a service that is rarely free for a client. A more secure remote banking could be more expensive for a client but will provide also some more secure e-commerce possibilities. We present in the next subsection some more details on targeted services by the SOPAS project.

Objectives

First, we have in particular to fulfill the client needs to use Internet to carry out its remote banking operations. Today, implemented solutions have the main drawback to be based on a password authentication that is not really secure (Pfitzmann et al., 1997). Thus, the SOPAS project has two major objectives:

- to gain the user's confidence;
- to provide a secure solution whose cost of deployment is as cheap as possible.

The client must be able to realize different operations such as those detailed in Table 1:

Table 1: Remote banking operations

Operations	Examples
Standard operations	Consultation, transfer, direct debit …
Credits	Consummation credit, real estate credit…
Assurance	Assurances subscriptions for automobiles, home…
Saving & Shares	Opening of a saving account, stock buying & selling

These transactions are very sensitive if we consider the financial impacts of an uncontrolled use. So, before any access to a banking site, a preliminary authentication is required. When the client is authenticated, the remote banking site proposes all the possible operations.

For certain operations realized by the client, it could be necessary:

- To protect against all alterations, the transaction exchanges between the client and the bank;
- To guaranty the good achievement of the transaction to the client;
- To have the client's agreement proof.

All that objectives (authentication, integrity, good achievement and client's agreement proof) can be realized by question/answer mechanisms:

- The bank generates a question and the client uses a personal device to generate an answer to the bank;
- The bank verifies this answer for the authentication process or to validate the transaction.

Second, one client must be able to make a payment on e-commerce websites in an easy and a secure way. We assume here that the merchant is 3D-secure compliant. This is not a strong hypothesis as it is supported by MASTERCARD and VISA.

General principles

We propose to use three elements in order to guarantee the client's authentication for remote banking and for 3D-secure compliant e-commerce:

1. smartcard: a client is also a cardholder. This smartcard is considered by the banks as very secured and have been personalized by the issuer bank with cryptographic keys to achieve many secure operations. The belonging of this smartcard and the knowledge of the PIN code by the cardholder gives some good guarantees for the bank issuer for its authentication.
2. Personal device: the personal computer is not a secure environment for a strong authentication of the cardholder. We propose to use a separate device as an interface between the smartcard and the personal computer. This personal device must be very secure and low cost. The solution is here to use a box just equipped with a 2x12 figure screen, a 4x4 keyboard, a card reader and no chip. It is the smart card itself which pilots directly the personal device by its I^2C bus and communicates with the personal computer by its USB bus. This solution is very different to the solutions which use a device which is able to compute. Here the “intelligence” and the security of this personal device is completely delegate to the smart card. When the smart card is not connected to the personal device, this one has no secret at all and can be produced everywhere in the word for a very low cost.
3. CAP (Chip Authentication Program) (MasterCard, 2004): CAP provides online chip-based cardholder authentication within the SecureCode™ program. It encompasses the chip application, the terminal, and the issuer server used in the authentication process, and the interfaces between these components. When the smartcard is slip in the personal device, the cardholder is invited to tape is PIN code on the keyboard. The PIN code goes directly to the smartcard and this one computes a token sent to the bank issuer via the personal device, the computer and the network without any modification.

Such a solution makes it possible to guarantee a complete security of the access to remote bank applications via Internet, ready to develop the confidence of the users.

The Figure 2 shows the SOPAS scheme for a remote banking application. The user has a SOPAS smartcard and a SOPAS personal device giving him access to the service. The user proves with the card that he is the legitimate cardholder by entering his PIN code. The card generates a token call “CAP token” which is used as authentication proof by the user to his bank. The token thus generated is transferred from the card to the user’s personal computer via the personal device, then, to the front end of the bank via the Internet network. This device is currently not used to require the user’s assent at the time of a significant banking operation (as in case of purchase stock for example). Indeed, the device would make it possible to seal a transaction; this seal is for the bank a proof of the user’s assent.

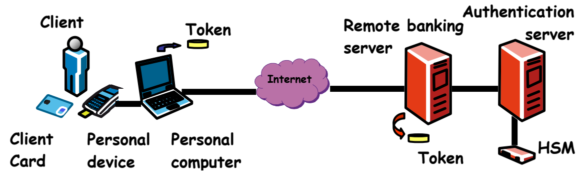

Figure 2: SOPAS solution for remote banking

The SOPAS solution is used mainly to authenticate the user to his bank. This solution, based primarily on the concepts of CAP authentication (MasterCard), should moreover be easily transposable everywhere in the world (see Figure 3).

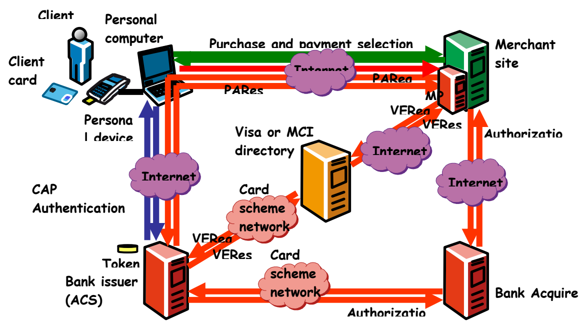

Figure 3: SOPAS solution for e-commerce

Interface protocols

The protocol used for the authentication is of challenge/answer type. The bank sends a random number to the card which turns over a token function of the received random number. This mechanism avoids the attack by replay, contrary to the systems of authentication having a static signature. Figure 4 illustrates the communication protocols used with the interfaces of the various entities intervening in the proposed solution.

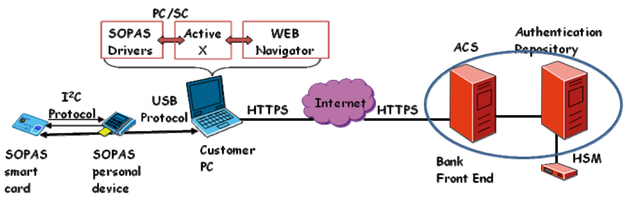

Figure 4: Interface Protocols

We can highlight the different parts of the figure 4:

- The SOPAS Card communicates directly with the personal device (equipped with a keyboard and a LCD screen) by a different interface than which is used to communicate with the personal computer. The protocol used is then I^{2}C (ISO, 1995). This is particularly important from the security point of view of the solution. This bus makes it possible the card to interact directly with its cardholder by presenting him some information via the LCD screen and while requiring some information (like his PIN code) via the keyboard of the personal device. These two operations thus do not require the intervention of the computer which is considered as a non secure element.
- The SOPAS card communicates directly with the user's personal computer with USB protocol via the personal device.
- The user's personal computer is exchanging information with the front end of the issuer bank using HTTPS protocol because the network is Internet.

Architecture

The following diagram (see figure 5) details the architecture and the relationships between the card and the personal device. We can observe that the USB and I^{2}C bus allows the card, either to communicate with the customer's personal computer via the USB interface, or to communicate directly with the personal device in order to reach its keyboard and its screen.

The second circuit (I^{2}C bus) strongly takes part in the security solution. The CAP token is calculated by the card, after the PIN code verification, then sends via the different devices without any modification and control to the HSM (Hardware Security Module) connected to the Bank Front End. So, only the two secure devices (Card and HSM) are able to calculate or verify the Token.

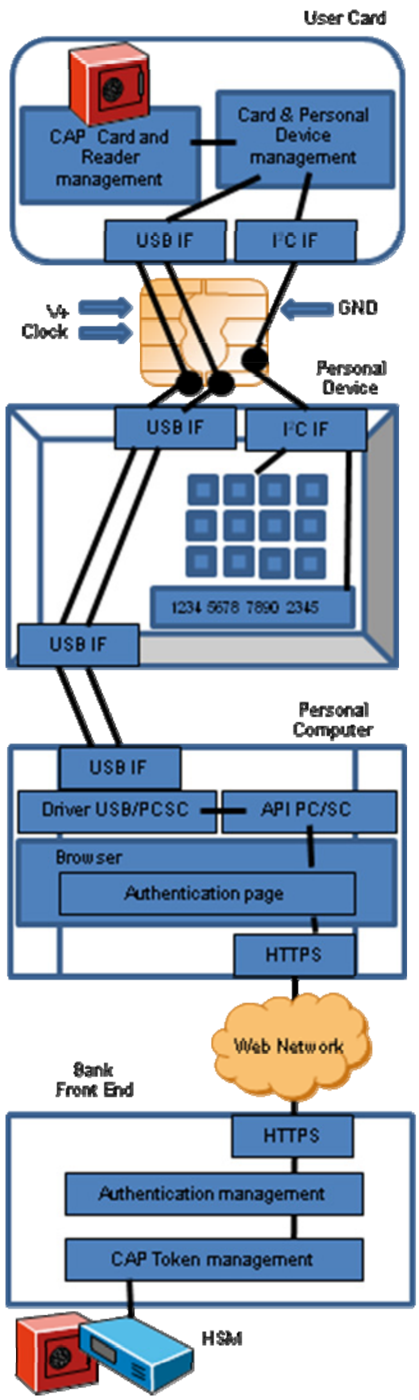

Figure 5: SOPAS architecture

SECURITY ANALYSIS

The objective of the section is to provide an analysis of the SOPAS solution as regarding the security aspects. We study the whole chain in order to determine the potential risks, then to provide some associated countermeasures. This analysis can lead us to possibly modifications of the specifications of the final solution. This is particularly justified by different attacks (phishing and pharming) against remote banking services and the different well known attacks in e-commerce and e-payment. We will endeavor to show that these attacks are completely identified within the framework of this analysis. It will appear that the SOPAS solution can then, in addition to being a solution of customer's authentication by his bank, can be a good solution for the bank authentication by the customer, making thus inoperative the previous attacks.

Methodology

To realize that study, we have used the EBIOS method (DCSSI, 2004). The card operating system answers the safety requirements evaluated according to common criteria (ISO, 2006). During the personalization of the card, the later remote applet loading is blocked. The card and the personal device are delivered by the bank, and the card delivery follows the standard bank card protocol (security requirement) and is delivered in a face to face situation by the bank. The delivering of the PIN is sent to the cardholder by the standard PIN mailer procedure.

Due to its cost, the personal device is an object which cannot be repaired and which is the subject to a standard exchange in the case of problems (in that eventuality the material is destroyed). The cardholder uses the SOPAS architecture in a personal environment and known conditions as standard use (for example without a company network environment…). The personal computer operating system is an area of risk whose protection is out of the study perimeter. The remote banking server (software and hardware) follows completely the security bank requirements. The bank is supposed to have correctly dimensioned and protected its architecture against mass attacks. The contract aspect between the cardholder and the bank must be reviewed by the bank lawyer and are not covered by this study. The SOPAS Smart card is not only a debit or credit card but includes also a CAP capability.

Results

The perimeter includes the following security domains:

- The user,
- The SOPAS smart card,
- The personal device (with its screen and keyboard),
- The link between the personal device and the client personal computer,
- the client personal computer,
- The bank server,
- The link between the bank server and the client personal computer.

The components, directly concerned by the SOPAS solution, appear in the top left hand in Figure 6. The total perimeter of the study is represented by an ellipse in Figure 4. The red entities inside the perimeter are those whose risks are excluded by the assumptions or whose countermeasures do not concern directly the SOPAS solution. For example, the SOPAS solution cannot ensure that the client personal computer is free from any virus software. In the same way, SOPAS cannot ensure that remote banking server is suitably configured, dimensioned... Nevertheless, for the red elements belonging to the perimeter, the analysis will be able, if necessary, to propose a countermeasure.

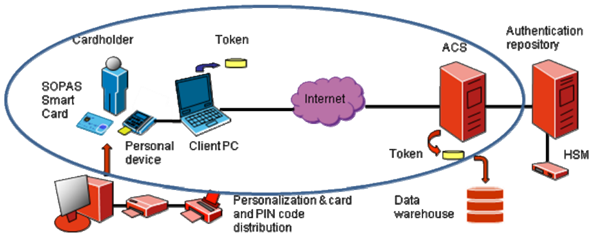

Figure 6: Study perimeter

The perimeter of this study integrates the data processing sequence of the authentication, from the card to the interface of the banking server. Before using the SOPAS smart card, procedures of personalization and distribution are necessary. Although, these last do not belong to the perimeter of the SOPAS solution.

The study of the vulnerabilities realized enables us to formulate a list of risks incurred by the essential elements. The transformation of these risks in scenario makes it possible to better apprehend them and judge their gravity. In this study, we formulate 19 risks. The majority of them concerns the banking data of the user or the technical information allowing the authentication of the customer by his bank.

The incurred risks are:

- The lost of availability ;
- The usurpation of identity ;
- The break of the RSA Keys of the SOPAS smart card (Anderson, 1994) ;
- The deterioration of banking data ;
- The disavowal of action ;
- The right abuse ;
- The divulgation ;
- The illicit processing of data.

During this study, a certain number of threats were identified. The threats which were retained are those which have a direct impact on the authentication mechanism. Additional threats, mainly on the remote banking server (except authentication function) were sometimes retained because it will have been judged that the SOPAS smartcard and the SOPAS personal device could thwart these last. They are mainly the threats and risks induced by the use of a personal computer to which remote banking services cannot grant its confidence. Indeed, it is not rare that the computer has been infected by a Trojan horse and became victim of the technique known as of the pharming.

It was shown during the study that the SOPAS solution makes it possible to cover the risks thus identified by associating to him a functionality of checking to a banking server certificate. That prohibits a fraudulent site to be recognized as being the bank. The user's personal computer not being confident, it is of primary importance so, on one hand, the checking of the server certificate must be embedded in the smartcard and, and on the other hand, the result of this checking must be shown on the personal device screen.

Finally, the risk of disavowal an action was retained because the authentication of a user does not have any value of assent on an action realized between the beginning and the end of connection. This implies the need for the user to sign each remote banking operations (of a sufficient amount). The signature functionality is in fact already present in the SOPAS smartcard but is just used for the user authentication by the bank.

This analysis also showed that, so far as we suppose that the user personal computer is safe (what is not the case but that nevertheless is posed like assumption), the encryption of the communications between the SOPAS smartcard and the user personal computer is not necessary. Indeed, the messages forwarding between these two devices are challenge/answer type, and are secured by that way. Coding from beginning to end would be a solution to mitigate the vulnerability of the personal computer which, by the presence of the malevolent programs, could deteriorate the banking data. This solution is however not realistic since at one time or another, the banking data must be posted on the screen of the personal computer.

To conclude this part, the SOPAS smartcard decreases the risks induced by the potential vulnerabilities of the personal computer. Indeed, the secrecies of connection of the user cannot be recovered any more by a simple keylogger or other spyware and attacks it by replay is not more exploitable. The use of a certificate embedded in the card and the checking of the bank certificate by the SOPAS smart card could further decrease the risks induced by phishing and pharming techniques. Nevertheless, the use of a personal computer that is not controlled (by the bank) remains the Achilles' heel of this service. Recurring problems here are found: how to protect data in an hostile environment?

CONCLUSIONS AND PERSPECTIVES

The SOPAS solution is made up of a personal device (card reader, screen and keyboard pilot via the I^2C bus by the card) and a smart card (Multi applicative card with the embedded SOPAS solution and standard EMV), the cost of the card is a little bit more expensive than a standard EMV chip card (6 to 8 €) but the personal device is very cheap (10 to 20 €). This makes it possible for the bank to deliver cards and personal devices to their clients interested for secure remote banking services and e-commerce.

Thus, the equipped user is able to generate a "CAP token" that he transmits to the bank like an authentication value, when he wishes to reach his remote banking services or to pay on the Web. The bank is convinced to deal with the good person because the smartcard, before generating the token, requires from the customer to enter his PIN code (known only by the card and the card holder), thus resolving the problem of the CAP token generation.

The security analysis of that solution shows that if we consider the limits created by the use of a unsecure personal computer, the SOPAS approach is a very good and secure solution compared to is deployment price.

There are some perspectives of this work. Two main changes are possible in order to limit the possibility for the user to repudiate his action:

1. To oblige the user to sign each remote banking operations (of a sufficient amount).
2. To use CAP Token generation options. In the Cap protocol, it is optionally possible to include the transaction amount and currency in the CAP transaction. This option is indicated by a flag in the card application, bit 8 of the IAF (Internet Authentication Flags).
3.

ACKNOWLEDGMENTS

Authors would like to thank all SOPAS project members: Alliansys, Credit Mutuel, Cartes Bancaires, Fime, Gemalto, the Basse-Normandie Region, and the French Ministry of Industry (DGE), for their kind cooperation.

REFERENCE

Anderson, R. (1994) Why Cryptosystems Fail. Communications of the ACM. pp. 32-41 ftp://ftp.cl.cam.ac.uk/users/ rja14/wcf.ps.gz.

DCSSI (2004) EBIOSV2: expression of needs and identification of security objectives

Ekelhart, A., Fenz, S., Tjoa, A.M., & Weippl, E.R., (2007) Security Issues for the Use of Semantic Web in E-Commerce. BIS 2007, LNCS 4439, Springer-Verlag, pp. 1–13

EMVCO (2000) EMV 2000 specifications. http://www.emvco.com/specifications.cfm

ISO (2006) ISO/CEI 15408 Version 3.1 Common Criteria for Information Technology Security Evaluation.

Kleist, V.F., (2004) A Transaction Cost Model of Electronic Trust: Transactional Return, Incentives for Network Security and Optimal Risk in the Digital Economy. Electronic Commerce Research, vol. 4, pp. 41–57

Konar, D. & Mazumdar, C. (2006) An Improved E-Commerce Protocol for Fair Exchange. ICDCIT 2006, LNCS 4317, Springer-Verlag, pp. 305–313.

ISO 7816 (1995) Standardization of smartcards

MasterCard (2004) Chip Authentication Program – Functional Architecture

Pfitzmann, A. (1997) Trusting Mobile User Devices and Security Modules. Computer, pp. 61-68.

Rennhard, M., Rafaeli, S., Mathy, L., Plattner, B., & Hutchison, D. (2004) Towards Pseudonymous e-Commerce. Electronic Commerce Research, Springer, vol. 4, pp. 83-111.

Visa Corporation. (2001) 3D–Secure Functional Specification, Chip Card Specification v1.0.

AUTHOR BIOGRAPHIES

Marc PASQUET is an assistant professor at ENSICAEN, France. He obtained his Master degree from ENSAM (Ecole Nationale Supérieure des Arts et Métiers) in 1977. He worked for 13 years for different companies belonging to the signal transmission field and 15 years for the banking sector in the field of electronic payment. He joined ENSICAEN (National Engineer School of Caen in France) in 2006 where he is now leading researchs in the field of electronic payment.

Delphine Vacquez is a Research & development engineer at ENSICAEN, France. She obtained her Master degree in 2006 from the University of Caen (computer science department). She has been working in the field of secure and contacless e-payment.

Christophe Rosenberger is a Full Professor at ENSICAEN, France. He obtained his Ph.D. degree from the University of Rennes I in 1999. He works at the GREYC Laboratory. His research interests include evaluation of image processing and biometrics. He is involved recently on e-transactions applications.