

Transactions Security and Payments via E-Commerce in Tunisia

Abderrazek BEN SALAH, Ph D.
E-MASIG - FSEGT Tunisia El Manar University
bs_abderrazek@yahoo.fr
+21620304647

Abstract

In Tunisia two intermediaries intervene during the execution of transactions and electronic payment, we will have two security policies in order to realize and guaranty the security of the electronic transactions. In Tunisia, e-commerce transactions are realized in two processes:

In the case of ONP (*ONP: Office National des Postes; NPO: National Post Office*) the security based on data cryptography and the secured connections where the merchant web site is totally implicated as all data pass through this site.

With the SMT (*Société Monétique de Tunisie, Bank Consortium*) the merchant web site is partially present during the transactions, and the client personal data do not pass through the site.

In the first process the client makes e-commerce transactions without knowing the intermediary of trust (ONP: Office National des Postes; NPO: National Post Office) has participated; In fact the latest was present only for the transactions guaranty, check up of both: (merchant site authenticity and the client's payment card) [9].

During the second process the client is directed toward the intermediary of trust just after having validated his on line purchase order, here intermediary of trust is SMT (*Société Monétique de Tunisie, Bank Consortium*), it simply takes the client into custody in order to guaranty the transaction.

As two intermediaries intervene during the execution of transactions and electronic payment, we will have two security policies in order to realize and guaranty the security of the electronic transactions.

In the case of ONP the security based on data cryptography and the securely connections were the merchant web site is totally implicated as all data pass through this site.

With the SMT the merchant web site is partially present during the transactions, and the client personal data do not pass through the site.

1. Introduction

The world existence is based on exchanges (all kind: services, products, goods and information) in all domains and thanks to the utilizations of computers and telecommunications networks the e-commerce is being a commercial reality that represents a considerable business revenue (more or less 300000 USD of international e-commerce turnover per minute).

This new fashion commerce will be an important tool in our daily social and business life likewise what the Internet has done to the world becoming an important communication tool between people and among companies.

The electronic commerce is being defined as the utilization of computer tools (hardware/software) and telecommunications networks (Internet in the reference network), in order to buy or sell goods, services of all kinds [1], [2], [3].

To realize this business exchanges (sell/buy) intermediary trust has to exist to guaranty the transactions that is being executed on the Internet [1], and not face to face as in the traditional transactions.

This intermediary of trust may be financial institution or an administrative authority has an important role to ensure the right and secured execution of the electronic transactions.

Tunisia was among the few African countries that stressed the importance of e-commerce transactions and the electronic payment via Internet and was also the first Arabic country which was connected to the Internet network [10].

The accessibility to the Internet was guarantied to a large number of Tunisians (at work/at home, 15% of population).

Universities and public administrations and especially private companies were the first to benefit from the technological infrastructure by creating their own web site (static than move to dynamic).

Banks and commercial companies are participating in this new way of communications in order to improve their customers services and to have a niche into the new electronic market [10, 11].

2. Secured execution steps of transactions and electronic payment between client and merchant

1. Visit of Merchant Web Site (MWS) and the choice of the goods/services, creation of the good's order page and the payment card type, information check up then order (on HTTP mode, shown on figure1).
2. TCP/IP connection of MWS through M Kit (plug in type, CGI scripts, installed by the ONP) with the main ONP server (Server Kit) on SSL [5] mode on private port and with data encryption (DES Data Encryption Standard - 1024 bits [5]) for: parameters exchanges between M kit and Server Kit,
- Merchant authenticity.
3. Server Kit response: - confirm if positive, otherwise cancel the connection.

4. Layout of web page on secure mode HTTPS thanks to a certificate bought from an electronic certification authority (International: Verisign, National ANCE: Agence National de Certification Electronique – NECA: National Electronic Certification Agency), encryption data RSA (Rivest Shamir Adelman – 128 bits [5]), to type the payment card number and the associated PIN code.
5. Read the screened information, and validate.
6. Insert data in the merchant data bases (without the client payment card details) in order to execute this purchase.
7. Forward of data toward the ONP payment server to execute the transaction.
8. Card and value validation request in E-Dinar data bases.
9. If the card is a bank card the ONP main server will ask for a check up from SMT server via secured private banking connections, on the other hand the SMT will use its own banking network for the same purpose.
The ONP may manage the Visa and Master card with special server that's verified by Visa.
10. The answer (confirmation or rejection).
11. Answer result:
 - a. wrong card number → retype the right number,
 - b. wrong PIN code → retype the right code,
 - c. not enough fund,

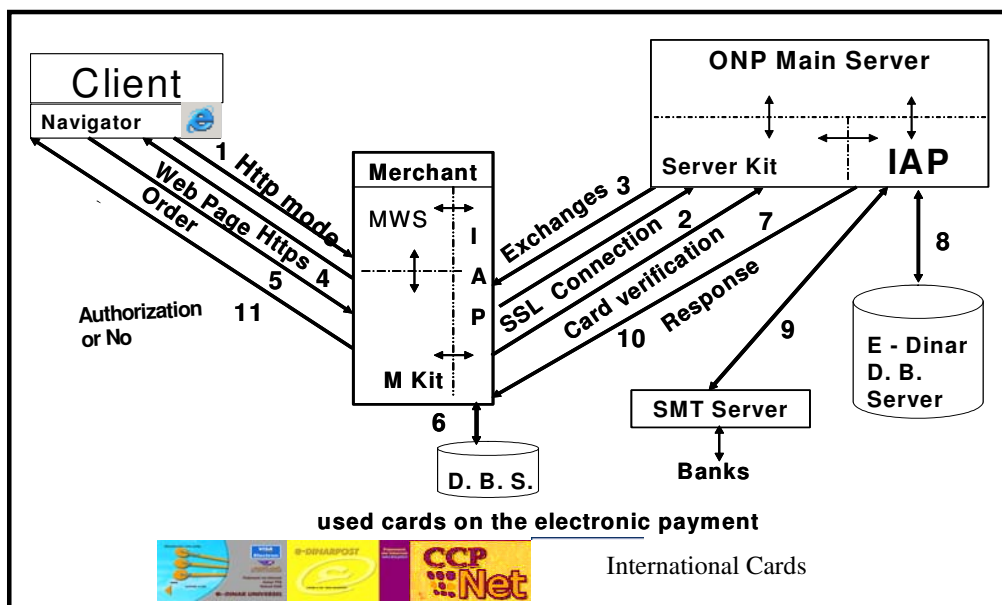


Figure 1. Secured transactions and e-payment processes between the client and the merchant via ONP

- d. transaction accepted, payment authorized. This page is a proof that the payment to the merchant was done (keep the print out of this page in case of conflict).
12. End of the transaction, the client is redirected back to the merchant site (this process is not shown on figure 1) as it has a marketing purpose to encourage the client to order more goods from this site.

3. The process authenticity of the Merchant Web Site by SMT

1. The validation of the client's order result in a payment request from the merchant to the SMT.
2. The Secured Payment Server (SPS) server checks the received information validity;
Valid information → payment authorization request,
Invalid information → invalid order (order cancelled).

With the call back method illustrated on figure 2, the SMT server verifies if the merchant web site server is the right one through inserted scripts on merchant web pages.

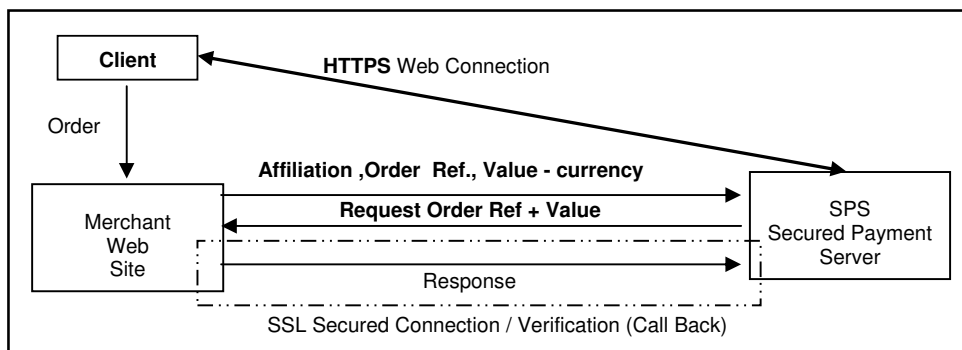


Figure 2. The process authenticity of the MWS by the SMT

4. Conclusion

The security systems of the ONP and the SMT are satisfactory. We have registered no fraud; on the other hand few complaints have been received due the connection problems and for bad utilizations in the different steps of the electronic payment transactions on the Internet.

Up to day, no serious hacker attacks to steal client's bank card details, this is explained either by the level of the hackers (not good enough to hack confidential data) or the security systems of ONP and SMT are good enough (this is confirmed by ONP and SMT systems operators).

However the level of security must still be tested by simulations of several serious attacks to finally say that the electronic payment transactions via Internet are viable.

5. References

[1] Kaplan Danielo, Guide du Commerce Electronique, SERVEDIT, 2000.

[2] Reboul P, Le guide du commerce électronique, Business Group. Publi-U-Edition, 1999.

[3] Reboul P., D. Xardel, Commerce Electronique, Editions Eyrolles, 1999.

[4] Langlois M., Gasch S., Le Commerce Electronique B to B de l' EDI à l' Internet, editions Dunod, Collection Internet Professionnel, 2d ed, 2001.

[5] Chernaouti-Hélie Solange, Sécurité Internet, Stratégies et technologies, , DUNOD , 2000

[6] Bordage Stéphane, Conduite de projet Web, Eyrolles, 2001.

[7] Monteiro da Rocha Philippe, Boutain Fabrice, Netentreprises réussir on line, Compus Press France, 2000.

[8] Danda Matthew, La sécurité sur le web, Microsoft Press. 2001.

[9] Rapport annuel de l'Office National des Postes tunis 2004.

[10] Loi n° 2000-57, modifiant et complétant certains articles du code des obligations et des contrats JORT n° 48 p. 1456, 2000.

[11] Loi n° 2000-83, relative aux échanges et au commerce électronique JORT n° 64 p. 1887, 2000.