SECURE E-BANKING IN GREECE

NIKITAS N. KARANIKOLAS[1]; GEORGE PENTARIS[2]

[1]Dept. of Informatics, Technological Educational Institution of Athens
e-mail: nnk@teiath.gr
[2]Commercial Bank of Greece
e-mail: pentaris.g@emporiki.gr

A Review of mechanisms for secure e-banking used by Greek Banks is presented. Some comparison, the common perceptions of security, the opposite directions and trends for future directions are also presented. We conclude with interesting deductions.

Keywords: e-banking, internet banking, mobile banking, security, OTP, PKI

1 REQUIREMENT AND AVAILABLE TECHNOLOGIES

During the last two decades banking industry has adopted new service channels. The most widely known are ATMs, Internet, Mobile and Phone Banking. In such widely accessed Banking environment, security is the ultimate prerequisite for establishing confidence to the alternative channels. There are a variety of technologies and methodologies that financial institutions can use in order to authenticate customers securely. These methods include the use of user names and passwords, personal identification numbers (PINs), digital signatures based on a Public Key Infrastructure (PKI), smart cards, one-time passwords (OTPs), transaction profile scripts, biometric identification, and others. Existing authentication methodologies involve three basic «factors»: something the user knows (e.g. password, PIN), something the user has (e.g. ATM card, smart card) and something the user is (e.g. biometric characteristic such as a fingerprint). Authentication methods depending on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed multifactor authentication methods are more reliable and stronger fraud deterrents.

The OTP solutions ensure that the password generated by the device (called token) is unique, unpredictable and different for every transaction. For the OTP choices we can mention Transaction Authentication Number (Wikipedia TAN) Lists, Short Message Service (SMS) OTPs (Allan et. al., 2006) also known as Mobile TANs (Weib, 2003), OTP Tokens, Smart Cards with handheld Readers (Todos TAN Reader), Credit Cards embedding OTP generation (InCard Technologies), etc. OTP Tokens produce one-time passwords, which are depended on two parameters. The first parameter is usually the tokens seed (credential) number and the second parameter is the time or some other challenge. Smart Cards with handheld Readers, also known as TAN-Readers, are also depended on two parameters. This solution has higher cost relatively to OTP tokens, whenever there is no prior investment in suitable smart cards (Allan et. al., 2006). The first commercial OTP Tokens were based on the Challenge-Response methodology. While reliable and effective, these tokens met a high degree of resistance in the market. In response to this resistance, the OTP manufacturers introduced the time-based tokens. These tokens removed the need of issuing a “challenge” by relying on time in order to automatically generate a password. The authentication server and the token have a shared secret (the token’s credential number). The token calculates a new random-looking value at regular intervals based on the shared secret and the time. As long as clocks are synchronized, the authentication server can calculate the same value. The recent introduction of event-based OTP tokens provides the advantages of time-based tokens and eliminates their associated disadvantages. Event-based tokens generate a new random password for each logon without suffering from time synchronization problems. However event-based OTP tokens suffer from the synchronization of the event counter.

PKI-based authentication (Wikipedia PKI, Allan and Litan, 2006) utilizes Digital Signatures, which are depended from PKI credentials and transaction details. PKI credentials are held either on a PC-connected smart token or on the customer's PC, using suitable client software. To create the signature the transaction details are hashed and the hash value is encrypted with the customer's private

key. From the other side, the bank obtains the customer's hash by decrypting the signature with the customer's public key and also generates its own hash of the transaction details. Then it compares its own generated hash against the customer's hash.

2 THE GREEK BANKS

We have investigated and briefly presenting the e-banking solutions of five Greek Banks: Alpha Bank, Commercial Bank of Greece, Eurobank, National Bank of Greece and Win Bank.

2.1 ALPHA BANK

Alpha Bank has invested in the two-factor authentication using the OTP token technology. Today the authentication of its e-banking retail clients is based on the OATH compatible (OATH) deployment of VASCO Digipass GO 3. It is a token with a simple touch button, which generates a unique one-time password, in every press. For its corporate customers, Alpha Bank invested to a USB token, manufactured by Gemplus (GEMPLUS), so that a digital certificate could be placed in it.

Alpha Bank's e-banking services are classified. Users can use Alpha Bank's information services and receive statements about the balance and the transactions for their accounts providing only their username and password. Providing also an one-time password the users are granted the right to perform transactions involving fund transfers. Moreover, when the fund transfers concern accounts of other banks, the clients should provide a fresh one-time password in every transaction. With regard to corporate customers, Alpha Bank imposes double authorization. One or more of the corporate users initiate the transaction and the legal representative user authorizes the transaction to proceed. The Bank perception of secure e-banking includes also filtered and monitored access to the Bank's systems, protected by the latest security mechanisms. Encryption is also used (SSL 128-bit).

For the future, Alpha Bank considers the incorporation of PKI technologies to its two-factor authentication. Other future mechanisms may include systems that will demand second level authentication (OTP, PKI, a phrase etc) not beforehand but only when the user's behaviour is abnormal.

2.2 COMMERCIAL BANK OF GREECE (EMPORIKI)

Currently, Emporiki Bank's e-banking system uses a single factor authentication based on the combination of a user id and a password. The bank has issued to its customers a high number of smart credit and debit cards. Emporiki Bank has decided to benefit from the distribution of these cards and integrate them to an One Time Password mechanism. The corresponding token (Todos eCode Signature) facilitates event-based mechanisms and smart cards in order to generate one-time passwords. Besides the event – based algorithm, the token also uses the secrets stored in the card chip in order to create and encrypt the password, which is displayed in the token's screen. After that, the user enters the password in an appropriate field of the e-banking application and it is transferred to the eCode server. The eCode server decrypts its input and performs a similar procedure to generate the one-time password. If this matches to the transferred one then the request is enabled.

There is an issue that needs some explanation. How the event counter is synchronized between the eCode signature (token) and the eCode server? The main cause for breaking synchronization is that the user can request a new OTP and never use it. The solution is to set a look-ahead parameter on the server. Synchronization of counters in this scenario simply requires the server to calculate the next event values that exist in the look-ahead window and determine if there is a match. The system may also require the user to send a sequence of OTP values for resynchronisation purposes.

A remarkable advantage of using smart card tokens is the simplification of the "logistics" concerning the distribution of the tokens to the e-banking users. There is no need for personalization of the token, as all required secrets (the event counter and the smart card keys) are kept in the smart card. This means that the user can obtain a token from any branch. The same customer can also use more than one token. At the first rollout of the new e-banking version, OTP will only be used as an additional security mechanism, for high-risk transactions. In the future, Emporiki Bank intends to use the eCode system for more complex forms of authorization, as Challenge-Response.

2.3 EUROBANK

Eurobank perceives on-line security as a very complex issue since it involves addressing potential risks, which can originate or manifest themselves from either the customer or the financial

institution. Therefore, Eurobank has been implemented a combination of technologies, policies & procedures, employee awareness and appropriate enabling organization to secure their e-banking environment. These involve Strict internal processes and security policies, Bank's website verification (via Certificate of Authenticity), Secured data transfers through encryption (128 bit SSL), User's authentication, Secured transactions through digital certificates (PKI), Further enhanced security in high value transactions through USB Digital Certificate tokens (Aladdin), Protected access to the bank's systems by the latest firewall technology, Intrusion detection systems, Virtual keyboard usage, Personalized transaction limits and Customized transaction workflows.

Another perception of Eurobank is that security cannot be complete unless the customer is aware of basic security behaviour to maintain secure the on-line transactions environment. Therefore, Eurobank aware its customers for safekeeping passwords, verifying websites and protect PCs.

Eurobank, the first and maybe the only Greek Bank engaged PKI, today has the perception that Certificates, especially hardware-based PKI, are the most secure way of doing transactions on internet, however it is less convenient. Now the perception is that security and friendliness should be well balanced. Their strategic decision is to increase the convenience and therefore the attractiveness of e-banking without compromising security by replacing the basic reliance on certificates with a mixture of technical, administrative and operational measures and techniques. At the same time the aim is to build customer trust and perception of security. In this direction, Certificates, OTPs and other identification techniques can be employed to customize appropriately the use of the e-Banking service. The Eurobank's new e–banking system, currently under development, is based on multi-channel architecture where all the above mechanisms are used together with revised transaction limits. Their plans include also adoption of real-time anti-fraud systems, which will analyse user's transactional behaviour and build personalized patterns, allowing real-time control of "suspicious" transactions.

2.4 NATIONAL BANK OF GREECE

National Bank of Greece (NBG) provides advanced methods of safeguarding transactions via alternative channels (Internet, Mobile and Phone). They cope with the security of all alternative channels in a united and uniform manner. The security policy that is being applied, guarantees the secrecy and inviolability in transactions. The parameters of security policy focus mainly on User authentication, Transaction authentication (with TANs and lately with OTPs) for each monetary transaction or when important elements are modified, Encryption of data (128 bit encryption), Bank's certification authenticity, Filters of access in the IT systems (Firewalls) and Personalized access / transaction control for corporate customers.

The recently introduced OTP devices of NBG are time-based and they are producing OTPs, which are active for only 32 seconds. For retail customers, NBG introduced the Vasco GO3 (Coresight) device (the brand name NBG uses is e-Code). For the corporate customers, NBG introduced the Vasco DP260 device. It is a small device with numeric keypad, simple 1-button operation and 8-digit LCD screen. The later device is PIN based, for the owner's safety. The owners can also change it at any time. The DP260 initially designed to support also two other functions: signature operation and challenge-response. The NBG considers the utilization of these functions.

NBG, in order to boost the sensation of security for its users, it confirms the transactions by sending back to the user a Host Authentication Code. The host code is a proof of identity of the central system to the user. By pressing once the button of the e-Code device, the user generates a one-time password (6 or 8 digits). The user enters the password to the central system for proofing his identity. The central system then verifies the correctness of this one-time password. If it is valid, the central system calculates the host code (3 digits). The host code is returned to the user who verifies if it matches the second part shown on his e-Code device (after a second press). Now the user is certain to be logged on to the correct Host and the Host knows to be in contact with the correct user. (Marinakis and Karanikolas, 2007) present the security of NBG's e-banking systems in more detail.

2.5 WIN BANK

Win Bank bases its two-factor authentication of customers in the OTP token technology. The RSA SecureID (RSA SecureID) time-based tokens that Win Bank users use to generate one-time passwords embody a USB connector and smart chip. The selected token is a lightweight and extremely easy to use token. It always displays a six digits OTP and without any user intervention (there is no

button) renew it every 60 seconds. The passwords can be used only once. Alternatively, Win Bank customers can get an OTP to their predetermined mobile phone number through SMS message.

Win Bank's e-banking services are classified. Users can use Win Bank's information services and also perform money transactions under an upper daily limit of 600 Euros providing only their username and password. For transactions ranging from 600 Euros to 7000 Euros OTP is required. For money transactions cross the limit of 7000 Euros a second OTP is required. The Bank's confrontation of secure e-banking includes also a fraud detection system that is developed in house (Aggelis 2006).

For the future, Win Bank considers the incorporation of PKI technologies to its two-factor authentication mechanism. Towards this vision, Win Bank made the right selection to use tokens that permit to add a digital certificate to the token.

3 CONCLUSIONS

Four out of the five banks we investigated are basing their two-factor authentication to the OTP token technology, while one out of five banks bases its security to PKI. All banks desire to be able to provide, in parallel with the currently used technology, alternative authorization methods. More specifically, in order to improve their security, two banks out of the four based on the OTP token technology have introduced, for their corporate customers, more sophisticated tokens. In one case the token can produce challenge/response OTPs and in another case a digital certificate can be placed in the token. The other two out of the four banks based on the OTP token technology have introduced from the beginning, and consequently for all of their Internet customers, tokens able to provide alternative authorization methods. In one case the token has the option to produce either challenge/response OTPs or event-based OTPs and in the other case the OTP time-based token can also host a digital certificate. The need for alternative authorization methods is also alive for the bank that bases its security to PKI. In that case the need comes from the perception that OTP tokens are more adoptable from the masses and especially from less educated customers.

Another remarkable point is that Banks are steadily adopting the fraud detection technology or improve their existing fraud detection systems. PKI obtain the interest of more banks but they are expecting to be set up a common PKI CA by the Hellenic Bank Association or some other Institution. As a final conclusion the alternative authorization methods, which banks aim to provide (challenge / response OTPs and PKIs), can satisfy the non-repudiation requirement (Tsai, 2002).

REFERENCES

1. Aggelis, V. (2006). *Offline Internet Banking Fraud Detection*, 1st International Conference on Availability, Reliability and Security (ARES2006), DAWAM Workshop, Vienna, Austria.
2. Aladdin. *eToken Strong Authentication and Password Management*, http://www.aladdin.com/eToken/default.asp
3. Allan, A., Heiser, J., Litan, A., Newton, A. and Wagner, R. (2006). *State of the Art for Online Consumer Authentication*, Garthner Research G00139254.
4. Allan, A. and Litan, A. (2006). *Transaction Verification Complements Fraud Detection and Stronger Authentication*, Garthner Research G00141750.
5. Coresight. *VASCO GO3*, http://www.coresight.com.au/vasco-go3-token.html
6. GEMPLUS. *ID & Security*, http://www.gemplus.com/pss/id_security/
7. InCard Technologies. *The ICT DisplayCards*, http://www.incardtech.com/products.html
8. Marinakis, C. and Karanikolas, N.N. (2007). *Strengthening the security of e-banking transactions. The case of NBG*, 11th Panhellenic Conference in Informatics, 2007, Patras, Greece.
9. OATH. *Initiative for open authentication*, http://www.openauthentication.org
10. RSA. *RSA SecureID*, http://www.rsa.com/node.aspx?id=1156
11. Todos. *eCode Signature*, http://www.todos.se/Todos/products/products_eCode_Signature.html
12. Todos. *TAN Reader*, http://www.todos.se/Todos/products/products_TANReader.html
13. Tsai, Chii-Ren (2002). *Non-Repudiation In Practice*, 2nd International Workshop on Asia PKI, Taipei, Taiwan, http://dsns.csie.nctu.edu.tw/iwap/proceedings/proceedings/sessionD/6.pdf
14. Weib, J. (2003). *Mobile TAN*, http://www.novosec.com/documents/eCommerce_MobileTAN_en.pdf
15. Wikipedia PKI. *Public key infrastructure*, http://en.wikipedia.org/wiki/Public_key_infrastructure
16. Wikipedia TAN. *Transaction authentication number*, http://en.wikipedia.org/wiki/TAN_(banking)