Strengthening the Security of E-Banking Transactions. The Case Of Nbg

Constantinos J. MARINAKIS[1] and Nikitas N. KARANIKOLAS[2]

[1] National Bank of Greece, kmarin@nbg.gr
[2] Technological Educational Institute of Athens, nnk@teiath.gr

Abstract

In this paper we describe the current situation, concerning alternative channels in security measures in the National Bank of Greece (NBG). We examine the need and the business motives for additional safety levels for the NBG offered services. We also examine the NBG decision and the advantages of the new two-factor authentication adopted. Some implementation details of e–Banking (Internet / Phone / Mobile Banking) are also presented and we conclude with a comparison with alternative potential solutions and future technology improvements expected.

Keywords: security, OTP, Internet Banking, two-factor authentication.

1. Introduction

During the last two decades Banking industry has adopted new service channels (alternative channels), based on technology progress. The most widely known are ATMs, Internet / Mobile Banking and Phone Banking. With the alternative channels a customer is able to perform banking transactions without his physical presence at the Branch and, very often, while being abroad. As a result, security is the ultimate prerequisite for performing successful operations and establishing confidence to the alternative channels customers. Security measures differ, according to each separate channel and follow certain rules established by each Bank, as a part of its security policy. Very often Banks should comply with regulations defined either from international organizations or from local authorities. Because of the many kinds of threats, which have been recently appeared on alternative channels, Banks are obliged to implement higher security levels.

Although National Bank of Greece (NBG) has adopted very strict security measures to all channels with extremely good results so far, it has recently proceeded to the establishment of a new two-factor authentication to strengthen the security of Internet & Phone Banking transactions.

1.1 Opportunities & Threats

According to the National Bank of Greece (NBG) main strategy, the Branch remains the main service point, with the alternative channels offering complementary services. Moreover, it is a strategic decision for the Bank to develop and enhance alternative channels in order to offer a wide variety of services to its customers.

Following this policy, NBG invested in Automatic Teller Machine (ATM) services many years ago, having the largest and most popular network in Greece. The ATM network offers quick Banking services daily, having a positive result in reducing queues in Branches.

Furthermore, the Bank started the first Internet Banking service 6 years ago. During all these years the IT systems have rapidly changed and a new generation e-banking system is being planned under portal technology.

During the last 2-3 years, many sophisticated threats have appeared, attacking ATMs with skimming devices and Internet users with phising techniques. As a result the Bank decided to strengthen its security measures. As regards ATM, an anti-fraud system has been established in order to monitor ATM transactions, with very good results so far. As regards e-Banking, a set of rules and measures is being followed, which are part of the NBG Security Policy.

1.2 NBG Security Policy

Recognizing the fundamental importance of security in executing electronic transactions, the Bank provides the most advanced and pioneering methods of safeguarding transactions via alternative channels (Internet, Mobile and Phone). The security policy that is being applied, guarantees the secrecy and inviolability in transactions. The parameters of security policy focus mainly on the following:

User authentication: It is the recognition of a user's identity by the system, so that it is ensured that only the authorized user has access.

Transaction authentication: The user enters a disposable number called TAN (Transaction Authentication Number) [Wikipedia TAN] for each monetary transaction or when important elements (e.g. change of password) are modified. If the requested transaction has been successfully executed, then the check TAN appears. TAN and check TAN numbers are printed on a sheet of paper called TAN list, supplied to the customer by his NBG Branch and should be safely kept. Each TAN code is unique, corresponds to a single TAN check and can be used only once. The production of each TAN is based on the 3 DES algorithm. Moreover, each TAN list uniquely corresponds to each separate user for safety purposes. This transaction authentication is still valid; although the Bank is in pilot phase with an improved solution using OTP devices (see §2.4).

Encryption of data: All information transferred from the customer's PC to the Bank (and vice versa) is purely confidential (using 128 bit encryption).

The Bank's certification authenticity: This is provided at the Bank site via Certificate of Authenticity, a certification published by independent companies - permitted for this aim. It ensures that no other can pretend to be the Bank and gain access to the user personal data.

Filters of access in the IT systems of Bank (Firewalls): hardware and software equipments are placed between the Internet and the IT systems of the Bank. It filters the entering data according to the policies of safety determined by the Bank's security group and the international models. Through this infiltration, all points of the Bank's network are protected in such a way that neither external nor internal unauthorized users have any access.

Access control for corporate customers: This can be achieved by differentiating each corporate user's profile and rights through definitions of category (A, B, C or D), mandatory transaction approval (level 1, 2 or 3) and by setting an amount limit for every monetary transaction.

1.3 Compliance Challenge

In the US, federal regulators are now requiring banks to have at least two-factor authentication with their websites by the end of 2006.

Greek Banks today face an increasing number of regulations that mandate the protection of information such as Sarbanes-Oxley Act (SOX) [Wikipedia SOX], Basel II [Wikipedia Basel II] and Bank of Greece directive [BG 2577].

The Bank's business problem is the need for a cost-effective compliance strategy which implements not only technical controls for information security but also policies, procedures and organizational changes as well.

Common practices across the regulations include: Authentication, Access Controls, Data Integrity Controls, Encryption, Audit Controls, Developing and Enforcing a Security Policy. Especially for the Access Control regulations, the Bank of Greece directive [BG 2577] suggests the usage of two-factor authentications and keep clear of transaction authentication methods that can suffer from phishing attempts.

The business impact is that failure to meet the requirements deadlines and on an on-going basis may result in penalties, shut down of operations, loss of customers and may damage the Bank's reputation by hurting the stock price.

2. Strengthen e-banking security

2.1 User's Authentication

There is a variety of technologies and methodologies that financial institutions can use in order to authenticate customers. 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), USB plug-ins or other types of "tokens", transaction profile scripts, biometric identification, and others. The level of risk protection afforded by each of these techniques varies. The selection and use of authentication technologies and methods should depend upon the results of the financial institution's risk assessment process.

Existing authentication methodologies involve three basic «factors»:

a) Something the user ***knows*** (e.g., password, PIN)

b) Something the user ***has*** (e.g., ATM card, smart card, security device), and

c) 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 and implemented multifactor authentication methods are more reliable and stronger fraud deterrents. For example, the use of a login UserId & password is single-factor authentication (i.e. something the user knows), whereas, an ATM transaction requires twofold authentication: something the user possesses (i.e. the card) combined with something the user knows (i.e. PIN). A multifactor authentication methodology may also include «state of the art» controls for risk mitigation (i.e. a security device generating one time codes).

The success of a particular authentication method depend on appropriate policies, procedures, controls and technology. An effective authentication method should have a customer’s acceptance, reliable performance, scalability and interoperability with existing systems and future plans.

Although most of the Greek financial institutions have not implemented two factor authentication yet, they offer an adequate security level in Internet Banking, with different implementations. Phone Banking is a relatively new alternative channel, offered by the most Greek Banks with a minimum set of transactions, under limited user authentication.

Conclusively financial institutions offering Internet-based products and services should have reliable and secure methods to authenticate their customers. The level of authentication used by the financial institution should be the appropriate for the risk associated with those products and services.

Although the NBG has already a two factor authentication for Internet Banking (UserId / Password plus TAN numbers), it has decided to increase security level by using special purpose security devices. This decision covers the security risk analysis results for the NBG’s new alternative channel: Phone Banking. In Phone Banking the Bank offers almost all the appropriate Internet Banking transactions by using the latest IVR (Interactive Voice Response) technology supporting speech commands recognition. Another motivation for the above decision was that there exists arguments [passivemode.net] supporting that TAN lists suffer from phishing attempts.

2.2 Moving from TAN list to OTP (e-Code)

The purpose of a One Time Password (OTP) [Wikipedia OTP] is to make it more difficult to gain unauthorized access to restricted resources. An unauthorized intruder given enough attempts and time can more easily access traditional static passwords. By constantly altering the password, as is done with one-time password, this risk can be greatly reduced. Moreover using OTPs, as the second factor in a two factors authentication schema, we eliminate security weaknesses. Using small electronic devices is the most popular (if not the only) way for producing One Time Passwords. The NBG’s brand name for the OTP tokens (devices) used in Internet and Phone Banking is e-Code. The advantages of e-Code against TAN list are the following:

a) Increase in transactions security level (each OTP is active for only 32 secs),

b) Simplification of the provided service (the issuer neither has to administrate the TAN list nor to assure their proper delivery, the customer has not to have the TAN lists on hand during transactions),

c) Decrease of the investment. Actually e-Code devices cost about $ 50 per item and the price can be decreased to $ 3 per item in case the bank purchases quantities in the range of one million items [Allan et. al. (2006)]. Therefore, the cost in the later case is affordable for the activity level of banks like NBG. The most important factor is that in case of computing gadgets there is a disposal for sharing the cost between financial institutions and their clients. On the other hand the TAN lists demand a considerable administrative cost (associate the TAN codes with the clients record, keep track for the utilization of every single TAN (used / not-used), issue new TAN lists, etc). Consequently, in the long run, e-Code devices present decreased overall cost.

d) Increased flexibility and quality in service (life expectancy is 5 years).

As a result, the use of e-Code not only eliminates possible difficulties in the customer service arising from TAN list (e.g. time delays, problems in the service of Internet Banking users who are non residents, permanent renewal of lists etc) but it also saves additional cost for the Bank (communication with the customers, postal expenses etc).

Even the non familiarized user, irrespective of age, can carry the e-Code device and with the push of a button can produce a disposable code, using Internet, Mobile or Phone Banking with any device (PC, PDA, mobile phone, telephone). The use of dynamic disposable codes renders any violation or interception practically impossible, because of an exceptionally limited time duration effect and an output (via powerful algorithms of encryption) by the device also based on the parameter "time". At the same time, special software in Host system of the Bank confirms the genuineness and validity of each dynamic disposable code. Obviously all the transactions (successful or not) are kept on an audit log.

Each token (device) is unique and personalized for each user / customer. Consequently, it is ensured that no third person has access either to the accounts or the electronic transactions (e-banking) even in the case of disclosure of a user's identification codes.

In our days there is a wide acceptance of OTP devices. Garthner in a recent article [Allan et. al. (2006)] make this clear "Despite the cost, this is probably the single most widely used method by banks in Europe, the Middle East and Africa (especially Benelux, Scandinavia and the Baltic) and Asia/Pacific (Australia, New Zealant and Japan). Use is still increasing, and many recent contracts each embrace several million retail customers."

For completeness reasons we have to mention the Short Message Service OTPs [Allan et. al. (2006)] also known as Mobile TANs [Weib (2003)]. This method delivers to customer's mobile phone an SMS message that contains an OTP, after the user enters valid identification items (UserId / Password). This method has two main weaknesses. The SMS coverage can be patchy in some areas, no guarantee delivered and customers may be charged for the SMS message. Another solution for OTP creation is Smart Cards with Handheld Readers, also known as TAN-Readers [todos.se]. This solution has higher cost relatively to OTP tokens (devices), whenever there is no prior investment in suitable smart cards [Allan et. al. (2006)].

2.3 Algorithms for producing OTP

The security devices offered by the supplier support a broad range of algorithms by which the response is generated. Each of these algorithms has its unique set of properties, allowing use of time, event or challenge based methods (or any combination of the previous parameters) in order to calculate the response (OTP).

Time-based operation: In the case of time-based operations, the security device allows you to choose between different granularities. The granularity indicates the frequency by which the response will change. When using the Time-Based Response only, the typical granularity is 36 seconds. This means that the security device will generate a new password every 36 seconds. Other granularities are possible as well e.g. 8 secs, 16 secs, 32 secs. Time-based can also be used in conjunction with challenge, e.g. performing a Time-Based Challenge/Response. This will prevent replay attacks for Challenge/Response authentication.

Event-based operation: The security device supports event-based (counter-based) operations, where the counter is incremented at every calculation (response generation).

Challenge-based operation: The security device supports challenge/response authentication. This can be compared with a question /answer scheme, where the server issues the challenge (question) which must be typed into the security device, which in turn will generate a response (answer) based upon this challenge. Challenge / Response is often used in combination with time, to prevent replay attacks.

Signature operation: Typically in banking applications the security device can be used to sign transactions, where the user is asked to type specific data in the transaction (e.g. destination account number, transaction number, amount, etc.). The security device will generate a response based upon these input parameters acting as a transaction signature.

2.4 NBG's selection – technical description

Based upon previous paragraphs conclusions, the NBG selected to implement the time based algorithm in every e-Code device. In the next steps we describe the total flow on e-Code usage.

At first the e-Code devices are initialized with their unique set of secrets and keys. These secrets are stored in an encrypted way on a CD that is sent to the NBG IT security department. The files on the CD will be used to deliver the necessary secrets and other data (i.e. serial numbers) into the Data Base. On every e-Code device the pre-initialized seed value and the time value are input to a 3-DES algorithm producing the dynamic password. The time is delivered from the Real Time Clock, internally to the e-Code device, which cannot be altered from the outside. Since DES is, by nature, a symmetric algorithm, the DES keys and other secret information needs to be present on the Host system for the verification process. After a successful verification between the e-Code device and Host, a special algorithm synchronizes the RTC gain or loss with the Host system time clock, based on a pre-defined acceptable time window.

Advantages:

- When OTP is used once, it becomes invalid and it is later invalidated by the fact that it falls outside the time window.
- Immune to replay attacks
- No risk of sync lost compared with event based synchronous system in particularly when taking full advantage of the time management synchronization functions.

- The time granularity was chosen to be 32 seconds, which is, according to NBG's measures, sufficient time to embed in the transaction.

Host Authentication Code:

The host code is a proof of identity of the central system to the user. After a dynamic password is generated inside the e-Code device (by pressing the button once) it is shown to the user as two different parts. The first part called the "password" (6 or 8 digits) and the second part called "host code" (3 digits). The user sends the first part to the central system for verification and for proofing his identity. The central system then verifies the correctness of this password. If OK, the central system calculates the second part of the password: host code. The host code is returned to the user who has to verify that it matches the second part shown on his device (by pressing the button for a second time). 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. By using the host code we minimize the risk of the user's connection being directed to a false Host.

3. Interaction with Users in Internet & Phone banking

3.1 e-Code distribution & activation

The customer completes an application form at the Branch office, requesting to be an e-banking user. The typical process ends when the branch clerk hands over the UserId and the e-Code device to the new user. The e-Code activation begins when the serial number of the device is associated with the UserId and both data are transmitted to the Host. The next day a password is mailed to the new user.

Existing e-banking users can visit any Branch and ask for the e-Code. The e-Code activation can be performed via Internet Banking or exceptionally by the Help Desk.

3.2 Using e-Code in Internet banking (incl. mobile)

A pair of UserId and Password are required for user authentication. The password usage obeys a specific security policy. After successful authentication the user (retail or corporate) is able to perform monetary or security handling transactions. The transaction data are sent to the central system with an OTP generated by the e-Code device as we later describe in detail (see §3.4). In case the user enters a wrong token the central system permits two more tries. After the 3rd wrong token the e-Code device is locked. The unblocking process is carried out in any Branch and by the Help Desk on an exception basis.

3.3 Using e-Code in Phone banking

A pair of a UserId (numeric) and an OTP are required for user authentication. After a successful entry the user is verbally instructing the system to perform a bank transaction. The completion of each transaction requires an OTP generated by the e-Code device as we later describe in detail (see §3.4). The e-Code device is locked after entering 3 wrong tokens. The unlocking process is permitted only at the Branch office.

3.4 Authenticating transactions

Our hope for mitigating the phishing threat is the mandatory use of two-factor authentication for banking systems accessible over the Internet or phone line.

An OTP is a non-repeating number generated by the e-Code device that changes every 32 seconds. The token generated by the e-Code device is of a dynamic nature, so it is only valid for a short period. This means that the attacker does not have very much time to use the token he has just stolen. So, the phishing attack actually becomes more difficult or even impossible. Two-factor authentication is much more than just the One-Time Password (OTP) technology. The emerging OTP technology protects against today's phishing attacks.

Above all the user is certain he sends the data to the correct bank: after the successful transaction the central system returns the Host Code, so the user can compare it with the one generated by the device.

Hence, it becomes clear that e-Code device technology authenticates every important factor, namely the user and the bank. This means that this technology successfully prevents all attack opportunities. Even more important, is the fact that the genuine user can conduct on-line transactions with his bank in complete safety.

3.5 Types of security devices

3.5.1 Security devices for retail users

Recently, NBG introduced the VASCO GO3 [coresight.com.au] e-Code device for the retail customers. It is a small portable device; dimensions approximately 12.5*30*60 mm; weight 10 grammars; simple 1-button operation and 8-digit LCD screen. There are also extra features such as an indication of the battery status level and the serial number.

The e-Code device’s serial number is associated with a unique UserId. Loss or theft of the device has to be reported immediately to the NBG’s Help Desk team (24*7 operation) so that can be immediately locked. Defective devices are immediately replaced at every Branch.

3.5.2 Security devices for corporate users

For the corporate customers, NBG introduced the VASCO DP260 e-Code device. It is a small portable device; dimensions approximately 75*46*13 mm; weight 28 grammars; with numeric keypad; simple 1-button operation and 8-digit LCD screen. The device is PIN based for the owner's safety. It lies in the user's responsibility to set on his first PIN. He can also have it changed any time he wishes.

The DP260 initially designed to support also two other functions: a) signature operation (see §2.3) and b) challenge-response (see §2.3). The NBG is under considerations for the utilization of these additional functions for securing alternative and/or complementary services.

There exist the same regulations for device's serial number and UserId association and for locking lost or theft devices. However, defective devices are replaced only in the central Branch. Since the device is PIN based the (remotely) assistance of Help Desk agent is needed for PIN unlocking.

4. Discussion

The main problem of TAN lists is that they are vulnerable to phishing attacks. This problem is solved with OTP tokens. However there are solutions that stand between the classical TAN lists and OTP tokens. For example, Plossl, Federath and Nowey [Plossl et. al. (2005)] propose a visual cryptography mechanism. According to their proposal the client is supplied with a challenge-response list (paper) and a transparency. When the client carries a transaction, he has to combine the list and the transparency to see the response that corresponds to the challenge provided by the bank. Oppliger and Gajek [Oppliger et. al. (2005)] present some other solutions that improve the security of TAN lists. The main idea under the later solutions is to protect the TAN lists in a way that reading a TAN require some physical action (rasp away a physical layer that hide a TAN) that can be detected if is done without authorization. These solutions seem to be less vulnerable to phishing attacks relative to classical TAN lists approach and moreover they don't impose any modification to systems already compliant with classical TAN lists. However, the NBG's vision / attention to the future, lead the decision to use OTP tokens.

Public Key Infrastructure (PKI) is the most promising technology for secure banking transactions. However the cost is very high, comparable to OTP tokens, and the mobility of the customer is very poor. Actually the usage of PKI is limited since it is characterized us not remunerative investment and demands customers with advanced culture.

As we have mentioned OTP tokens completely remove the risk of phishing attacks. However, there is still the Man-In-The-Middle danger, which is coherent with web spoofing [Wikipedia SA]. Of course the duration of 32 seconds of each OTP decreases the danger but it is not completely removed. There are a lot of proposals suggesting mechanisms to decrease this danger. The Browser-Side Protection Mechanisms [Oppliger et. al. (2005)] suggests improving future browsers in ways that prevent tampering of the Browser's Security Connection Indicators (BSCIs). As an example future browsers must permit the user to apply his own background bitmap to the padlock indicator. As a consequence the user will be able to distinguish between authentic and web spoofed communications. The Interaction Protection Mechanisms (for example the Delayed Password Disclosure) are also effective to counteract to web spoofing attacks [Oppliger et. al. (2005)]. The above-mentioned mechanisms detect web spoofing and prevent the Man-In-The-Middle danger before it happens. However, there are mechanisms, for example the Transaction Anomaly Detection [Allan et. al (2006)], which detect in progress Man-In-The-Middle fraud transactions.

5. Conclusions

Although NBG had implemented e-banking services that are sufficiently secure, it recently made a decision to adopt new emerging technologies and strengthen the security of its e-banking services. In its security strengthening decision NBG didn't adopt solutions that are improvements in its previous investment in classical TAN lists and preferred to adopt the world wide acceptable solution of OTP tokens. However, NBG didn't adopt PKI, which is the pin point of technology, since there is no wide acceptance. Since the adopted technology does not completely absolve from the Man-In-The-Middle danger, NBG should observe new emerging technologies against the mentioned danger and adopt them as complements to its robust secure e-banking solution.

References

Allan A., Heiser J., Litan A., Newton A., Wagner R. (2006), *State of the Art for Online Consumer Authentication*, Garthner Research G00139254.

BG 2577, *Bank of Greece directive 2577.*

coresight.com.au, *VASCO GO3*, http://www.coresight.com.au/vasco-go3-token.html

Oppliger R., Gajek S. (2005), *Effective protection against phishing and web spoofing*, in 9th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security.

passivemode.net, *Online Banking Transactions*, http://passivemode.net/updates/2006/10/12/online-banking-transactions.html

Plossl K., Federrath H., Nowey T. (2005), *Protection Mechanisms Against Phishing Attacks*, in Trust, Privacy and Security in Digital Business, Lecture Notes in Computer Science Volume 3592, Springer.

todos.se, *Todos TAN Reader*, http://www.todos.se/Todos/products/products_TANReader.html

Weib J. (2003), *Mobile TAN*, http://www.novosec.com/documents/eCommerce_MobileTAN_en.pdf

Wikipedia SOX, *Sarbanes-Oxley Act*, http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act

Wikipedia Basel II, *Basel II*, http://en.wikipedia.org/wiki/Basel_II

Wikipedia OTP, *One-time password*, http://en.wikipedia.org/wiki/One-time_password

Wikipedia TAN, *Transaction authentication number*, http://en.wikipedia.org/wiki/TAN_(banking)

Wikipedia SA, *Spoofing attack*, http://en.wikipedia.org/wiki/Spoofing_attack