

# TellerPass

by Yiannis Hatzopoulos  
Scientific Engineering Services  
[www.ses-ltd.gr](http://www.ses-ltd.gr)

**Abstract:** TellerPass is a 3.5kbyte SIM Card applet for GSM phones, which dynamically generates cryptographically secure PIN passwords that get changed every 30 sec, and are used only once. These PINs can be utilized to access bank accounts through ATM kiosks, or web-banking and phone-banking sessions.

TellerPass is engineered to run in-synch with banking login servers, using an autonomous and link-free architecture. PIN generation and check is performed using synchronous distributed digital signatures. TellerPass bypasses the man-in-the-middle attack shortfall of conventional hardware OTP (One-Time-Pin) generators, by utilizing the wireless network.

TellerPass applets from many different banking issuers can co-exist securely inside a SIM card, adding a strong layer of security in the administration and use of multiple banking account PINs.

In many countries, bank ATM machines strictly accept magnetic stripe cards. On many occasions, fraudsters have successfully tapped ATM card inserts, red debit card's IDs, captured the owners' PINs using micro-cameras or mock keyboards and built counterfeit cloned debit cards; extracting money from the owner's account using another ATM, even from across the globe. Tourists using ATMs in Southern Europe and the Balkans have been especially vulnerable to attacks; although many of them use dual access smart-card / magnetic stripe debit or credit-cards to withdraw money from ATMs, most of the local ATMs only employ the cards' magnetic stripes. PIN recording and playback is a common attack method and a major problem for banks and their customers. A similar case occurs in web-banking. Attackers try to capture login names and passwords to devoid accounts from cash using spyware keyboard grabbers, phishing sites and social engineering scams.



Banking institutions fight-back by selling 'key-chain-lock' security tokens to their clients - like the one which is depicted bellow from the National Bank of Greece (under the brand name eCode). These are battery powered devices with a tiny LCD screen and one button, which when pressed, displays for 30 sec a six digit time/date bound PIN password, to enhance the security of web-banking sessions. The eCode PIN is used as an additional check to the user's normal PIN.



*(eCode key-chain-lock banking token)*

The web-banking application expects to be given this 30 sec lasting PIN to grant you access to your account. Banks charge around 7-12 Euros for this secure device. Not all users opt for this, due to cost and possible inconvenience; this is understandable when one has to juggle with more than 2-3 bank accounts and needs to carry around tokens from different banks, since these systems do not interoperate, so as not to compromise security. Even carrying around two of these in your key chain lock is a major discomfort. Believe me, I tried it and I know what I am talking about! ECodes eventually run out of battery and need to be replaced (that means buying a new one) every 2-3 years. Even this piece of technology presents serious weaknesses and does not really protect from a man-in-the-middle attack, masked over a well designed phishing site.

ATM users on the other hand are left unprotected and are advised by banks to keep a watch-full eye for fraudsters when they use an ATM machine. Upgrading an ATM network costs big money, thus banks simply prefer to postpone it! It is also a well known fact that ATM users do not change their PINs - and sometimes even write them on their debit cards, so as not to forget them, especially when they use several of them. Clearly this is a recipe for disaster!

A cellphone would be the ideal platform to base our solution and most precisely a cellphone SIM card, which is universal, hosts a secure set of keys inside it, can perform crypto -math, can do one-way hashing and can receive accurate time/date info from the mobile network. The solution- a cheaper, more practical and versatile alternative to the eCodes of this world, has been named TellerPass – a mobile dynamic PIN generator, which presents some quite interesting features:

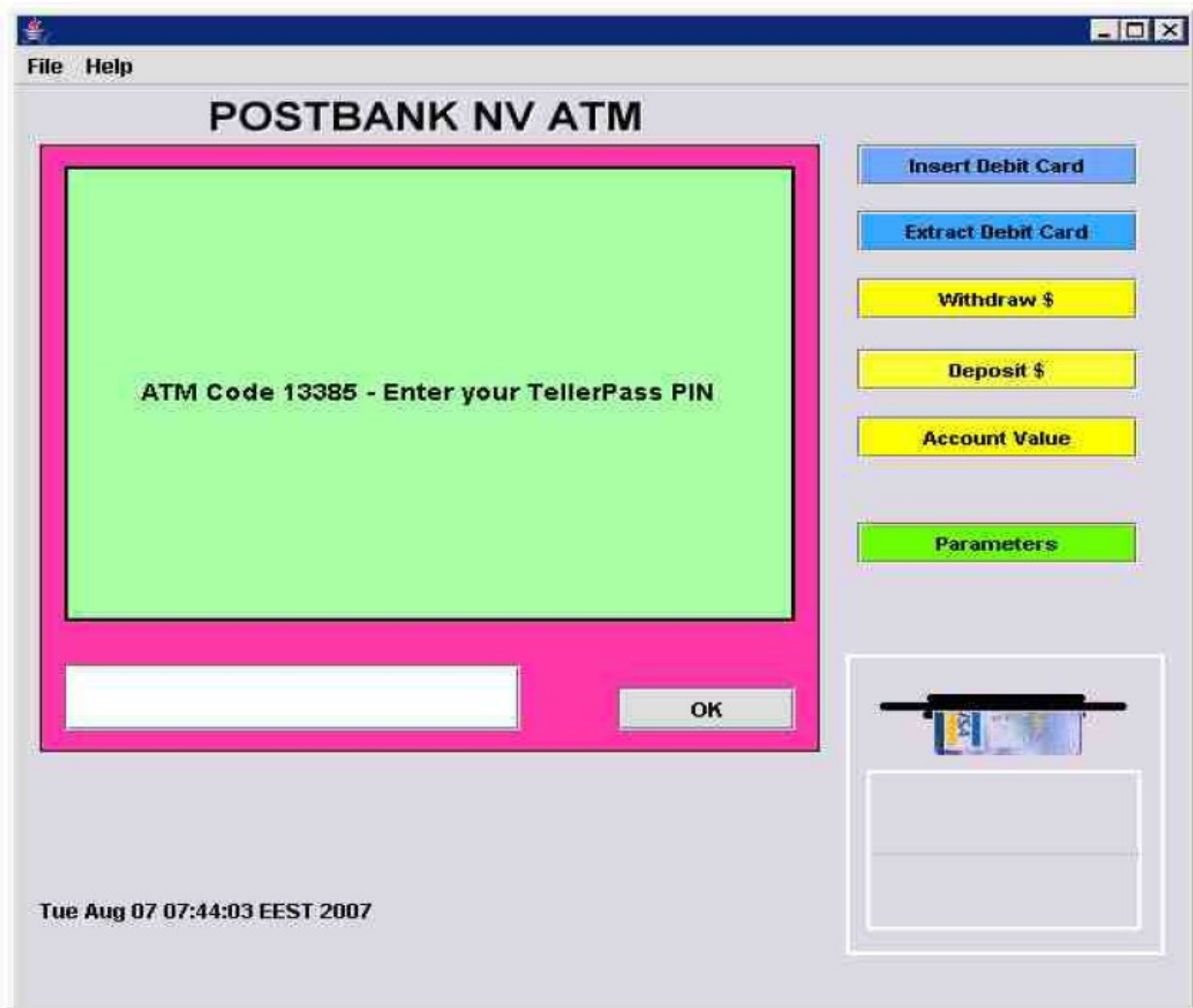
- TellerPass is password protected by the cellphone.
- You can have many TellerPass applets from different banking issuers in your cellphone. This is very convenient. A 32 Kbyte SIM card could safely host 2-3 PIN generators, leaving adequate space for other applications.
- One TellerPass applet can be used both for ATM, web-banking and phonebanking access (DTMF touch-tone access to account).
- A TellerPass applet can be downloaded and made available to the cellphone instantly, the moment the user opens an ATM / web-banking account and at no significant cost – typically less than one Euro.
- When the user changes his phone, or his phone gets lost or stolen, with just a phone call to the bank, his active TellerPass applet can be invalidated and a new TellerPass can be downloaded to the replacement phone.
- Further down the line, TellerPass, could be an alternative to debit card based transactions at ATM kiosks. Simply Identify yourself at the kiosk with an ID number that you read on your cellphone's screen, give the ATM the one-time PIN that is generated by TellerPass and you will get immediate access to your cash, without carrying a debit card with you. It is actually the principle “Something that you have – something that you know” that grants you access to your account.
- TellerPass is actually running 'off-line'. No interaction and communication with an OTA server is necessary during its operation, which obliterates any chance of eavesdropping and removes telecommunication charges, both for the bank and the user. This feature becomes more significant as the user count grows. The security of the keys involved is guaranteed by the SIM card itself.
- A TellerPass user does not need to remember any banking PIN codes altogether, if he chooses to do so.

## Usability and interface

From a usability point-of-view, the user interacts with TellerPass in the following manner.

The ATM user inserts his debit card in the card insert slot; the ATM immediately recognises that this customer is a TellerPass user. Optionally, a 5 digit number is projected on the ATM kiosk's screen (ATM

check code) prompting the user to enter this number as a launch code in his TellerPass application. Since most ATMs do not perform a video capture of their user, this is an additional security feature, which helps to certify that a legitimate user is present in-front of the ATM, and not somebody spoofing the transaction. The user runs TellerPass in his cellphone , types the ATM suggested launch code and presses the OK button. One second later TellerPass responds by displaying on the mobile's screen a 5 digit PIN password which is valid for 30 sec. The user enters this TellerPass dynamic PIN on the ATM kiosk's keyboard and is immediately granted access to his account. This dynamic PIN is automatically invalidated following its 30 sec life-span.

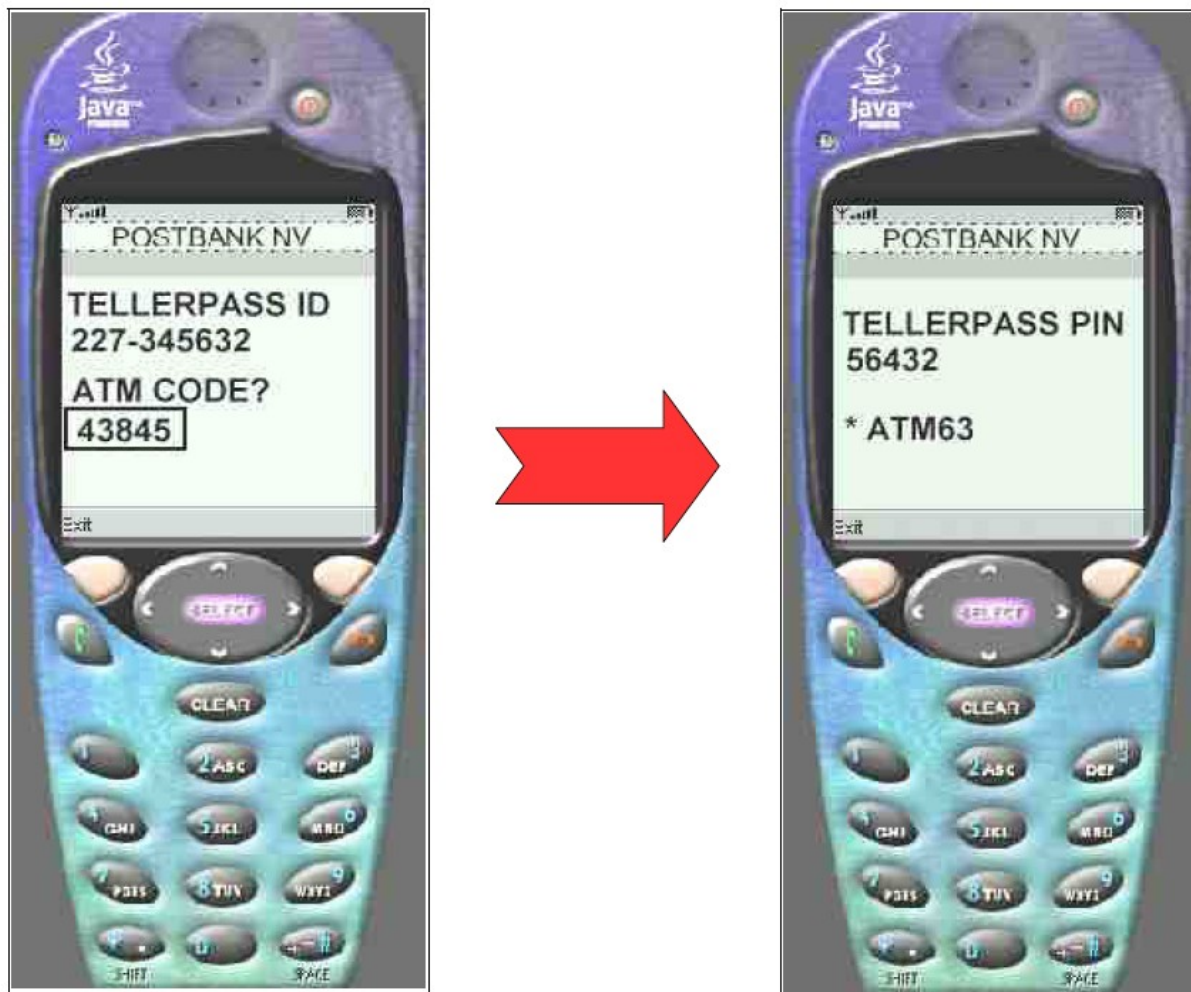


*(a snapshot of our TellerPassATM demo)*

Should the user need to use the ATM at a later time, a new TellerPass dynamic PIN must be generated. The total amount of time required to run the applet, enter the optional launch code and receive a dynamic PIN is less than 10 sec. TellerPass is a password protected SIM application,

although the user can disable this protection, simply relying on the cellphone's SIM card PIN code protection.

A similar process would grant the user access to his web-banking or phone-banking account. In the latter case, telephone DTMF touch-tones could be used to submit the user's ID and TellerPass PIN to the service, through the phone's speaker, before the system allows connection to a human phone-teller operator. In web-banking, to invalidate any potential of man-in-the-middle attack (through a phishing site, to which eCodes are still vulnerable to), the TellerPass applet can be configured to send its dynamic PIN automatically by encrypted SMS to the Login server, using a toll-free number.



*(TellerPass dynamic PIN generation interface)*

Any critical operation such as money transfer, payment, buying/selling stocks over the phone or the web, could be verified by a dynamically generated TellerPass PIN password. Even if interactions with the ATM or the web server are being recorded, the fraudster would have no way to

replicate the transaction process and launch an attack.

The scam would be immediately identified.

Along the PIN, a two digit ATM return code is also projected on the cellphone. This helps to identify mock-ATM (yes! mobsters have built some of these) or fraudster eBanking web-sites. If the transaction return code on the ATM does not match the cellphone's, it is a clear indication that we are channelling our transaction through fraudstermedia. In this case, we should communicate immediately with our bank to freeze our account. TellerPass could be utilized as an ever-changing electronic verification signature in many e-applications and foremost in credit-card ePayment platforms. Don't forget that TellerPass works off-line and it is autonomous.

Most importantly, a cellphone SIM card could host multiple TellerPass applets issued by many different banks, without compromising each-other's security. Should an organisation opt to download employee SIM cards with TellerPass, the employee cellphones could be used to generate dynamic PIN passwords necessary to access computer network resources or even deactivate electronic locks. Indeed the sky is the limit...

Having described the user interface, it would be quite interesting to discuss how this miniature application works. TellerPass and the Bank's ATM login server use a shared secret to provide security. TellerPass is downloaded wirelessly and is installed on the user's cellphone just like any other sim-card applet. Immediately afterwards, TellerPass generates a Public-Private key pair inside the SIM Card. TellerPass sends its public key with an SMS message to the OTA server. The OTA server sends back an SMS message containing a secret bank-assigned subscriber ID, encrypted with the TellerPass public RSA key. TellerPass receives this encrypted SMS message and decrypts it with its private key. It retrieves the secret subscriber ID that the bank has assigned and a displayable TellerPass ID. TellerPass stores both keys safely inside the SIM card. In the test application we have submitted, we used the standard mobile network DES encrypted SMS delivery, which is adequately sophisticated to demonstrate the secure delivery concept of the secret subscriber ID to the cellphone.

Alternatively, a bank might opt to send this data in writing by registered post-mail to the user. The user would just have to type the data manually (usually a 16 digit number or 128 bit key) on his cellphone. As a secret number, a bank could equally well utilize the user's current 'static' bank account PIN; the user will enter it once in TellerPass, which will in turn get it transformed into a dynamic PIN. There are so many different options

that every possible security strategy can be accommodated.

The TellerPass applet synchronizes its internal real time clock every time it is launched. From the stage of passively receiving the network's/phone's timestamp, TellerPass does not use any kind of interaction with the mobile network. During the actual monetary transaction, to enhance the security, we can ask the user to enter in his TellerPass cellphone a 5 digit number that is projected on the kiosk's screen or the web-banking login service (ATM check code – different in every transaction); we call this random number 'ATM seed'. (This is an optional feature, to make sure that the user is physically present in front of the specific kiosk or IP address designated, and not spoofing the transaction).

## Time-clock granulation

In the TellerPass time-world, the real time clock of 24 hours is granulated in 2880 halfminute slots, which are used in our time calculations to allow our distributed system to work even if the clocks of the login server and the user's cellphone ( or mobile network's ) fall slightly out of synch. Thus our mathematical time unit is a 30 sec time unit.

At this stage we have the basic components we need to set up a shared-secret platform check between the bank's login server and our cellphone, without using an intermediate live communication link. It is all based on simple mathematics, XOR reasoning, one-way secure hashing algorithms and modulo operations. Of-course this description is only meant to demonstrate the concept. Additional complex mathematical permutation formulas would be used in a real application setting to make mathematical attacks and reverse engineering infeasible.

To demonstrate this concept, the following simplified mathematical formulas would yield a secure 5 digit PIN that lasts 30secs :

**(128 bit Secret SubscriberID)  
bitwise XOR (64 bit current granulated mobile network GMT  
time\_date stamp) bitwise XOR (40 bit ATM seed projection  
number) = rawPINData  
SHA-1(rawPINData) = 20BytePIN\_A  
SHA-1(20BytePIN\_A) = 20BytePIN\_B  
(20BytePIN\_B) modulo 65352 = PIN**

The same set of calculations is executed by both the SIM card and the Bank's ATM login server. We want the executable code in TellerPass to be as simple as possible; therefore the mobile network's timestamp (local time always) is normalized into GMT time inside the TellerPass applet.

The current ATM login server timestamp is always in GMT. Thus, we use a compatible time-frame reference, regardless of time zone (e.g using an ATM in a foreign country).

The Login Server performs the above calculations based on the current GMT date-time timeslot, the previous one( -30sec) and the next one (+30sec), to allow the user a 90 sec transaction accessibility window. In other words, the Login Server will accept 3 possible PINs that respond to three half-minute timeslots (sliding time window) along the current GMT time; and since the same GMT reference is used by the cellphone, the transaction will work from any location in the world. This sliding window provision is necessary to compensate for network delays introduced in the ATM authentication and communication with the banking servers.

Don't forget that each time-slotted PIN will only be accepted once by the Login Server and for 30 sec; Each PIN is dependent on the current ATM-Code, the shared-secreted subscriber ID and the current GMT timestamp; thus no clock forwarding attack is possible and no fraudster attack can be based on any previously used PIN code.

## Practicability and business aspects

TellerPass is a mass market mobile application. It strong-holds over an established hardware base, the SIM card, and aims to provide to cellphone users a fuss-free security gadget that will make their transactions with universal eBanking services bulletproof and transparent. TellerPass addresses security lapses that cost international banks and their customers millions of Euro in damages every year. ATM and web banking attacks cause an even greater damage to the image of banking establishments. The necessary software development from a bank's side is rather minimal and is estimated to cost no more than two man-years per implementation (mainly due to back office database integration services and ATM login server extensions involved). The transmission and installation of the actual 3.5 Kbyte TellerPass applet to a cellphone would cost something in the area of 0.10€/unit in bulk volume.

This prototype is in early stage development, and to be able to comment further on its business aspects and its marketability would be difficult, as additional testing and feedback would be required from potential users. Efforts will be made to liaise with people from the banking and transaction processing industry to assess the technology and its implications. \_