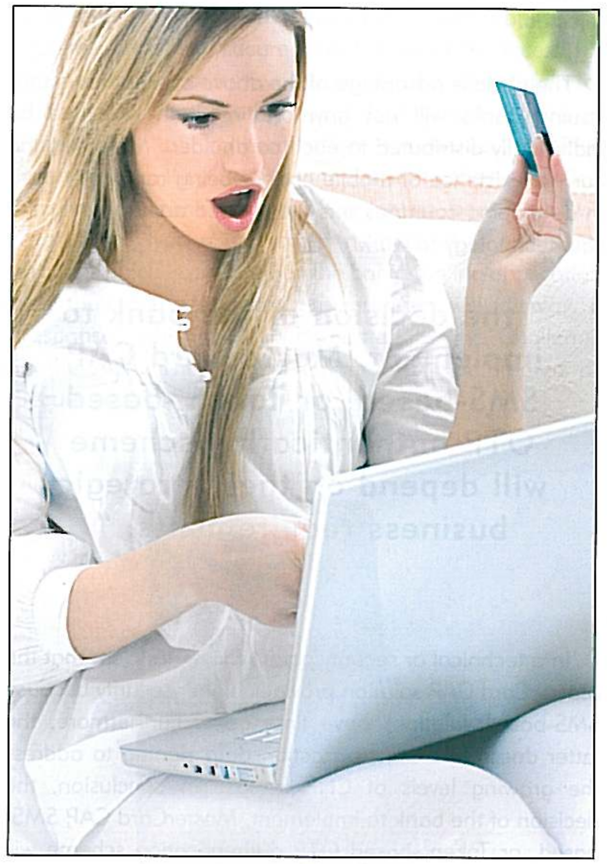
HOW TO INCREASE THE ONLINE-BANKING USER'S CONFIDENCE?

By Mr. Gilbert Leung Advanced Card Systems Ltd.

Online banking (or Internet banking) allows customers to conduct financial transactions on a secure website operated by their bank, credit union or building society. Online banking offers users the facility to monitor all their accounts because features such as bank statements, electronic bill payments, fund transfers, loan applications, loan transactions, and account aggregations are being provided. It is widely recognized that online banking provides more revenue per customer and costs less per transaction than any other banking channel.



However, according to the annual figures released by the Association for Payment Clearing Services (APACS), online banking fraud losses in the UK - one of the European countries that is aggressively implementing home banking, reached from £22.6 million in 2007 to £52.5 million in 2008. In other words, there is a whopping 132% increase caused by fraudulent transactions alone. Other headline figure comparisons between the years 2007 and 2008 statistics include an 18% rise in counterfeit card fraud to £169.8 million; a 39% jump in card ID theft to £47.4 million; and a 13% increase in the card-not-present fraud to £328.4 million [1]. The said figures of the online banking fraud losses have been without a doubt a major reason why the delay of online banking service deployment is inevitable. Therefore, it has also been a pressing issue between the bank executives and their corresponding IT department on how to provide solutions to increase the confidence of the e-banking users.

Despite pessimistic statistics, e-banking has an extremely bright future due to its rising popularity and the escalating number of online services offered by banks globally. However, maximizing the potential of e-banking requires the financial institutions to overcome one of the most troublesome obstacles ever faced in the industry: identity (ID) theft. ID theft has affected nearly 27.3 million US consumers and leads annual losses of US$50bn in the US alone [2]. One of the possible solutions to address the said problem and the growing threat of fraud is to implement a MasterCard CAP (or Visa DPA) application.

MasterCard CAP program

MasterCard introduced its Chip Authentication Program (CAP) (and PINless Authentication (PLA)) applications to the banks in order to reduce the fraud from "Card-not-Present" (CNP) scenario. These applications provide a mechanism and standard for securing online transactions. Sub-licensed by Visa, CAP and PLA use the cryptographic functions available on an EMV compliant bank card to provide core security during cardholder authentication. The advantage of MasterCard CAP is that it supports three types of authentication methods:

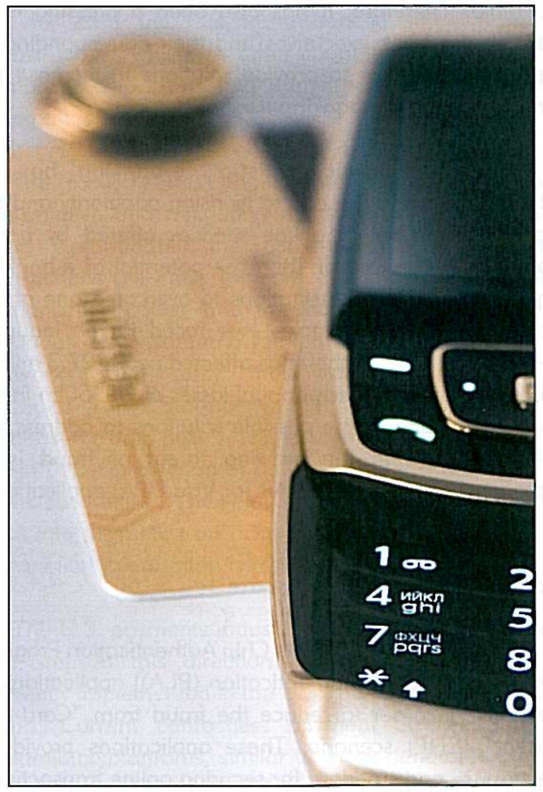
(1) Identify - the Authentication Card Reader (ACR) engages with the EMV compliant card to produce a "Secure Code" which is then used by the cardholders, for example, to log into a banking website.

(2) Response - this is a "challenge-response" mode where the issuer asks the cardholder to enter a challenge number into the ACR which then generates a response number. The response is used by the cardholder to authorize log in or verify a transaction.

(3) Transaction data signing - this mode is an extension of the "challenge-response" method, where in addition to entering requested challenge data in the ACR, the cardholder also inputs transaction specific data i.e. amount, currency etc. [3].

MasterCard CAP VS other alternatives

Despite all of the advantages of the MasterCard CAP, some banks consider using other Two-factor authentication (TFA) alternatives such as the SMS- or OTP token-based authentication.



If the bank has access to the mobile phone numbers of the cardholders, SMS-based authentication can offer a convenient and inexpensive way to communication through real-time authentications of transaction between the clients of the bank and their mobile phones. Most of the SMS messaging services are operated using "Pull messages." These messages are initiated by mobile phone users who are also clients of the bank for the purpose of obtaining information or performing a transaction of their bank accounts. For example, a unique One-time password (OTP) is requested by customers each time they want to perform transactions using the online banking platform. When the request is received, the OTP will be sent to the customer's cell phone via SMS. The password is expired once it has been used or once its scheduled life-cycle has expired.

On the other hand, if the bank is implementing an OTP token-based authentication solution, it has its advantages and is also commonly used. This method can be done by a variety of authentication processes such as an event synchronous or a time synchronous scheme. In an event synchronous scheme, the OTP token is generated each time they are activated (usually by pressing a button). The generated OTP is then compared to another OTP generated by a back-end server using the same crypto algorithm with keys and an incremental counter. While a time synchronous scheme has a unique OTP generation every particular time.

In theory, the event synchronous is less secure than time synchronous because a hacker (who has gained access to one of these tokens) can temporarily generate a sequence of OTP's that can be used later on. "OTP" as the name implies can only be used once for authentication verification process. Otherwise, if the OTP is recycled for another authentication verification event, it will be rejected.

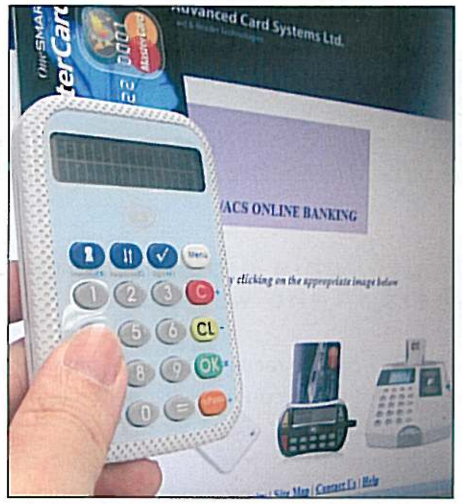
The obvious advantage of the above alternatives is that issuing banks will not anymore invest in ACR's to be individually distributed to each cardholder. Moreover, the current existence of mobile phones being rampantly used in developing countries sets the needed apparatus for the said technology to work.

> **" the decision of the bank to implement, MasterCard CAP, SMS-based, or Token -based OTP authentication scheme will depend on their strategic business requirements. "**

In a technical or security point of view, it's clear that the MasterCard CAP solution provides higher security because SMS-based solutions have time gaps. Furthermore, the latter doesn't have a transaction data signing to address the growing levels of CNP fraud. In conclusion, the decision of the bank to implement, MasterCard CAP, SMS-based, or Token -based OTP authentication scheme will depend on their strategic business requirements.

MasterCAP compliant Authentication Card Reader (e.g. ACS APG8201)

Nevertheless, Authentication Card Reader (ACR) is one of the major elements of any MasterCard CAP/PLA programs. APG8201 is one of the available EMV CAP readers in the market. The online bank user inserts his EMV compliant bank card into ACR and enters his PIN via the keypad of the ACR. Once the PIN is confirmed and verified by the offline PIN stored in the bank card, the ACR will generate a unique one-time "secure code" which will be entered by user when the online bank application requests. And this "secure code" is used to access his personal bank account information and do certain of transactions. On the other hand, if the bank requires a higher level of authentication for some sensitive transactions, they would implement the so-called "Challenge-response" mode. The online bank user will be asked to type a challenge (normally it is a 6 digits numeric) which is provided by the bank's online application over their website. Then, the reader will display a "Response" which will be generated by the Challenge via the ACR. Then, this "response" will be treated as "Secure code".



Conclusions

When the banks or organizations are considering implementing a strong online authentication solution, they have to think about different aspects, such as security level, deployment implementation, ease of use, manageability, and scalability. While the "Identify" and "challenge-response" modes are commonly used and are widely accepted in today's market, they can easily be applied to all types of CNP transaction scenarios. Although this process only authenticates the cardholder, it doesn't secure the transactions being processed. Hence, this leads to identity theft and the so-called "man-in-the middle" attacks which is on the rise. Malicious attacks can occur by obtaining or intercepting sensitive information (e.g. account numbers, amount of money being transferred, etc) during a real-time transaction between a user's PC and his/her bank. Therefore, the transaction data signing mechanism is very important to alleviate this vulnerability.

> **" When the banks or organizations are considering implementing a strong online authentication solution, they have to think about different aspects, such as security level, deployment implementation, ease of use, manageability, & scalability. "**

From my point of view, the market should adopt the MasterCard CAP technology widely. It is also possible for banks to take advantage of implementing MasterCard CAP for online authentication applications and use other alternatives such as SMS for over-the-phone transactions. That way, they will be able to exploit the obvious security advantages of different technologies while keeping their future options open.

However, customer's education is vital. A good example of why education is so important is phishing. A bank can invest a lot and implement the best technology, but the best way to combat phishing is through communication - similar to parents teaching their children proper manners. Banks need to educate their customers on how to identify e-mails that might be fraudulent, and also other security threats.

References

(1) Online banking fraud soars in UK, http://www.finextra.com

(2) Online Banking: Creating Confidence Through Security. Chen Arbel, Aladdin Knowledge Systems - 19 Feb 2008

(3) Chip and PIN: Complete Fraud Solution or Just One Piece of the Puzzle? David Dix, Cryptomathic - 18 Mar 2008

For further information please visit www.acs.com.hk