



**Gilbert Leung**  
Sales Director  
ACS

## Tackling Security Theft In Online Banking

Over the years, the banking industry has experienced an increase in the adoption of online banking among banking customers. Banks themselves promote online banking services over other banking channels since it generates more revenue per customer and maintains the least cost per transaction. Its overhead costs are lowered since customers no longer depend on personal branch banking. As for the customers, they avoid long queues inside the branch and evade banking hours. With a computer and an Internet connection, accessing a banking account to check bank statements, paying electronic bills, applying for loans and more, is possible anytime and anywhere for customers.

However, there are certain security risks that hamper the full deployment of online banking. With the availability of financial information online, crime groups have transitioned to adopting savvy technology to infiltrate online banking systems and steal online identities (ie. the username and password of an account). Phishing and Trojan virus schemes are 2 common and pervasive methods they use to perpetuate identity theft in online banking.

Currently, SMS-based and token-based One-Time Password (OTP) solutions are the most popular and widely adopted methods by the banking industry to reduce fraud in online banking. SMS-based and token-based OTP both utilise OTPs or security codes for accessing online banking websites, in addition to usernames and traditional passwords. SMS-based OTP generates a transaction-specific OTP that can only be used once. When unused, the OTP will expire on schedule. While convenient, this scheme is prone to hacking, since information transferred through handsets is not encrypted. Likewise, the system will only work after a thorough identity verification of each mobile number's owner.

Meanwhile, tokenisation generates OTPs either on a time-synchronous or an event-synchronous scheme. The former generates OTPs every given time period, whereas the latter generates an OTP on every click of the device's button. Since they are not transaction-specific, these schemes are not effective in completely preventing Card-Not-Present (CNP) fraud. Not only can hackers gain access to the token in an event-synchronous scheme and generate OTPs that will be considered as valid, Trojan viruses directly working on the customer's PC can also exploit a time-based OTP in use within a certain period. Given the pros and cons of the 2 solutions, banks' choices are limited to considering between a tolerable level of security risk on their part and a tolerable level of inconvenience on the part of customers executing extra measures for securing online banking.


At the core of these security threats lies a vulnerability that cybercrime groups exploit - no physical use of bank cards is required during online banking service process. This leads to CNP fraud, in which fraudsters only need stolen online identities to perform fraudulent transactions. Hence, it becomes a top priority for the banking industry to employ stringent security measures to prevent these CNP scenarios and render phished or stolen identities useless. Only by countering these security threats can an optimal adoption of online banking be realised.

### MasterCard CAP And PLA Or VISA DPA Programme

Primarily designed to reduce cases of CNP fraud, MasterCard's Chip Authentication Programme (CAP) and PIN-less/Person-less Authentication (PLA), and Visa's Dynamic Password Authentication (DPA) scheme provide a strong mechanism and standard for securing online transactions. They provide the core security in card authentication by utilising the cryptographic keys embedded in the contact chip of every EMV card. Under this programme, the EMV-compliant card is complemented by an Authentication Card Reader (ACR).

Among the available ACRs in the market, the APG8201 and APG8202 Dynamic OTP Generators developed by ACS are 2 devices certified under the CAP/PLA/DPA programmes. Both utilise two-factor authentication where the cardholder is required to insert an EMV card (something he has) into the device and enter a PIN code (something he knows) using the built-in PIN pad. After successfully verifying both the card and PIN code, the device generates and displays a dynamic OTP via its LCD, and this OTP can only be used once for each online transaction.

Both the card's sensitive information and the cardholder's PIN code are securely limited and authenticated within the offline device, making it impossible for them to be hacked. Also, missing one of either the 2 factors prohibits the cardholder from proceeding with the transaction, thus CNP fraud is bypassed. Furthermore, the devices support the challenge-response mode for transactions requiring higher level authentication. Transaction data signing can also be applied to validate the transaction's authenticity.

Two-factor authentication is currently the most effective solution in curbing security threats to online banking. With the addition of smart cards into the equation, like using the EMV card with an ACR, two-factor authentication gains a more solid security foundation. Experts predict that the current design of smart cards makes them likely to provide a high level of fraud protection. In effect, this raises the dependability of two-factor authentication, which relies on smart card mechanisms. Perhaps it may not be the ultimate future of online security, but it will remain to be one of the most viable solutions for many more years to come. 

### Contactless Payment - powered by Morpho



Sagem Orga is now Morpho!

Sagem Orga (Singapore) Pte Ltd  
Phone: +65 6511 4360,  
Fax: +65 6274 5352

SAFRAN  
Morpho

[www.morpho.com/e-documents](http://www.morpho.com/e-documents)