



One Time Password – NOT just another application on your cell phone

By William Holmes, Consultant to GO-Trust



William Holmes

Suddenly there has been a rush to add numerous applications to Cell Phones and PDA's. These applications are most frequently social or inconsequential and are also most never business 'Mission Critical'. Mission Critical applications need something more than a software applet that runs on the cell phone (in the open), they need special secure hardware so that critical keys, seeds and calculations are never accessible and certainly never in the open.

But let's start at the beginning and briefly describe the One Time Password (OTP) concept. Static (user generated) passwords are vulnerable. The vulnerability could be something as simple as someone looking over your shoulder or a more sophisticated method like keyboard logging. Passwords may be left inside memory after logout and can easily be found by scavenger bots. Deduction based on the users preference and personal records (birthdates, pets' names etc.) and brute-force attacks are just a couple more of the methods to find out fixed passwords.

Then the almost obvious idea arrived, if you use a password only once it does not matter if it has been copied or deduced, the previous password has no value – One Time Passwords were born. As they are only valid for a single session or a single transaction they are not vulnerable to replay attacks. There are three common types of OTP algorithms:-

HOTP – Where the H stands for HMAC, which in turn stands for Hashed Message Authentication Code. This is a seeded algorithm that generates a series of unique passwords. The sign-on server is always looking for the next password in the series. As the algorithm uses a crypto hash function it is believed to be impossible to reverse engineer the series to calculate the next password.

TOTP – Where the T stands for Time-based. In this algorithm the real-time clock is an additional parameter. Generated passwords are only valid at a specific time and only for a defined time period.

OCRA – Where the acronym stands for Onetime Challenge Response Algorithm. In this algorithm the addition factor is a challenge code from the logon server.

Great idea, but there is an obvious snag; OTPs cannot be memorized by human beings and preprinted sheets of future passwords defeat the whole concept of unpredictable password series. The next obvious step was the development of standalone key generators. These key fobs and less frequently smart cards became very popular with financial institutions and multinational corporations. Simple to use and many times more secure than personnel remembering (weak) passwords.



Looks like a good solution but there are some downsides. The key fob is yet another thing to carry but more seriously it only has a two to three year battery life. Before that time is up there needs to be a total redeployment, the replacement of every key fob in the field! Smart cards are easier to carry, do not have batteries, but do require either a portable reader or a conventional smart card reader on a PC or notebook.

To recap, OTP is many times better than static passwords, but extra hardware is required to generate secure passwords, the current key-fobs and smart cards are not the ideal solution.





Last year in June 2008's SCN newsletter (<http://www.smartcard.co.uk/archive/>). I wrote about 'Smart Card Security for People and Applications on the Go' which detailed the latest technology to embed smart card chips in MicroSD memory modules delivering smart card, hardware based, security for applications on cell phones and PDA's.

This technology has moved on very quickly in the twelve months since that article with many new smart cards being available in the microSD form factor delivering new smart chip, hardware based, security to cell phones and PDA's. One chipset that has caused particular interest is the microSD JAVA, with EMV, Common Criteria compliance and FIPs certification. The flexibility of such a secure environment lends itself to an array of secure applications on mobile phones and PDA's, some of the more interesting include mobile TV, banking and secure VPNs.

Back to OTP, the microSD JAVA is the perfect platform for secure one time password generation. It is fast, easy to install in any phone or PDA with a microSD memory slot and it is completely secure. Unbelievably the microSD with the embedded JAVA chip still has up to 4 GB of flash memory most available to the user only a small amount is used to store the phone side display application. Installing the OTP application on your phone is simple:-

1. Insert OTP microSD into mobile phone SD slot.
2. Use the file explorer or a similar tool to locate the memory card.
3. Select the correct folder for the platform (Blackberry, Symbian, Mobile, Android) in the memory card.
4. Execute the file in the selected folder.
5. The Mobile phone will install OTP application and will be ready to run.
6. And running the application is even easier:
7. Select the OTP application from the main menu.
8. Select Generate OTP Value.
9. Input the PIN for the smart card chip embedded in the microSD.
10. The OTP is generated.



OTP Application Menu



The OTP Value

So why does it make sense to move the OTP generation to a Mobile Phone or PDA? Firstly the security is as good as it gets. Smart Card hardware security with EMV, Common Criteria compliance and FIPs certification. It is always right next to you, nothing else to carry or remember. There is no need to change your OTP system every two to three years as part of a mammoth redeployment of units. It follows your lifestyle, change your phone and the OTP application on the microSD moves with you. You can even use a full size SD adapter and run the OTP application on your desktop or notebook. The OTP application has not robbed you of your extra memory; the 4Gb of flash memory is still there on your phone for music, photos or data.

OPT will be the most secure, most valuable and most important applications on your cell phone!