



Smartcard Security for People and Applications on the GO

By William Holmes, Business Development Consultant, GO-Trust.



William Holmes

Everyday new features are being added to our mobile phones and PDAs. Some of the more obvious are cameras, GPS, Bluetooth and the most all encompassing; access to the Internet. Along with these features comes a myriad of new services, on-line banking, streaming video, mobile TV, micro payments, route planning and music downloads, to name just a few. Unfortunately these new services can also bring potential threats. There are several viruses already attacking mobile devices. There is the Cabir strain that is spread across mobile phones using Bluetooth. It is currently believed to be harmless but for how long will that stay so. Another virus called Mosquito arrives as part of a downloadable game. It compels phones to send text messages to premium-rate numbers without your approval or knowledge.

There's Brador (the Paris Hilton nightmare), which deletes files, resets your phone and sends contents such as an address book, e-mails or photos to a third party. So just as your office, home or notebook PC's are vulnerable to malicious and criminal users so are your mobile devices, only they do not have the array of security products available for your PCs, to protect them. Even the few that are available are rarely used.

There are many security challenges that impact the private and the business mobile user. First and obviously there is all your personal data; telephone numbers, calendar, photos, voice notes, and even very sensitive personal or business records. Then there is the actual communication itself; voice and text. Most data that is communicated from your cell phone or PDA is in the open. With the right listening device it can easily be intercepted, overheard and recorded. The financial services transactions are many and varied, banking, stock trading, small payments/prepayments in a stored purse. Business transactions can be anything from simple enquires about a product description, to highly sensitive, mission critical transactions concerning major sales or acquisitions. Media user authentication, copyright protection, distribution and storage are also all major issues. Taken altogether the security challenges are huge, and mostly neglected. One good thing from a security point of view, browsers on cell phones and PDA's do support SSL for encrypted transaction data passing between the client and the server.

To protect the integrity of most online services, it is almost always the same sign-on technique, source recognition (SiteKeys), usernames and passwords. Is it used because it is the best or because it is OK but cheap and easy to implement? I believe it is the latter and here are some of the limitations. A password is a shared secret that at least two people must know, so by definition it is vulnerable. The only authority, to say it was you who signed in, is the service provider and there is nothing you can do to prove irrefutably that it was or was not you making the transaction. Passwords are not usually ideal in structure. If you have to remember a few - especially on the go, when you can't look up the 'post-it' note in the top drawer of your desk - then you will usually keep them simple or at least easy to remember. That makes them much easier to deduce. As Microsoft says in its Security advice to small businesses use complicated passwords for any online sign-ins and change them regularly. Easier said than done. Combining fixed identification information from your mobile unit, will not solve the problem. If it is a fixed identity that can be read, then it can be cloned, just like any magnetic stripe card.

That is why hardware security devices (like smart card chips) are so effective. They cannot be cloned, the data they use for identification cannot be uploaded and the on chip processing cannot be observed by any other processes. With an encrypted challenge and response, particularly in a PKI environment you get very secure authentication. Even if your application still uses passwords, now you can store complex character strings or password sequence generators on the chip that can only be accessed when you enter your PIN. But a PIN is only a simple password, I hear you cry. True, but a hacker needs to have direct access to the chip and even then he only has a very restricted number of attempts before the chip automatically disables itself. The same is true if anyone tries to physically tamper with the chip. Chip are so powerful that whole applications can be run on them with the associated data kept in secure encrypted vaults. With security chips you have secure clients that protect the user information and data. They can also protect third party data like copyrighted text, pictures, audio and video. These units are not difficult to use and in most cases are almost invisible to the user. Security modules are wonderful devices so why aren't they everywhere on mobile devices?





They just don't fit the mobile device technology model. Smart cards with their readers or USB dongles are too large and both of these need additional, currently unsupported interfaces. So they fail the 'on the GO' test, they are not aesthetically pleasing, they require extra equipment, they add to the unit cost. Mobile devices are manufactured in their millions and their initial selling price is kept to a minimum and there is considerable pressure not to add to the unit cost. It looks like this is the end of the road for the smart card chip in the world of the mobile phone's and PDA's. It has been in the past; but not any more.

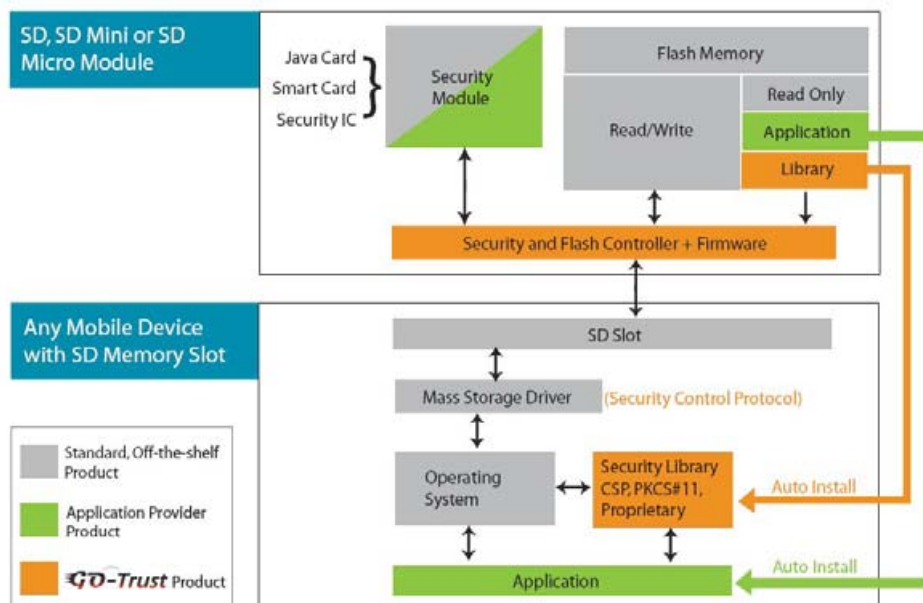
Most mobile devices have an external memory card slot, most commonly this is a SD slot. If you build the smart card chip into the SD memory card and also use the flash memory to store the security application, there are no longer any 'show stopping' technology model problems. The mobile device looks exactly as it did before, it has not required any additional interfaces or equipment to be built into the base unit, or changes to the operating system and it does not change the basic sales cost.

Any mobile device that has a SD memory slot can become a GO-Trust SD Secure Client. The security capability that is added is a strong hardware based security. There is nothing the user has to do other than insert the GO-Trust SD Solution card. A Cell Phone, PDA, Note Book PC, Tablet PC, (Even Desktop PC), Mobile TV, Portable Ultrasound, Digital Camera, Digital Camcorder, MP3/MP4 Players, Digital Picture Frame, GPS, Graphing Calculator, Wii Game System and many many more can now have hardware based security solutions.

'Security based applications' aren't all boring application that protect your assets working invisibly in the background. Some can open up completely new opportunities. For example planned applications require the digital media created on a mobile device like a camera or a video camera to have a non-repudiable origination verification from digital signatures or watermarking. Features like this are currently only available on the most expensive special built commercial units. If it was more readily available then cameras in car could irrefutably record a video of the last few minutes in front and behind your car. How valuable in an accident! Or any photographer could embed his copyright, location, time and origin in every photograph he takes at the moment it is taken

GO-Trust does not make the smart card chips or develop the security applications, we facilitate adding them to SD memory chips (standard, mini or even micro) so existing security applications can be made available easily on the billion plus mobile devices that have SD slots today. The user devices need no changes and remarkably the existing security applications can be migrated without redevelopment. Too good to be true – not after you see how conceptually easy it is.

It is a combination of three great technologies united on a SD memory card. Any manufacturer's security module plus any developer's security based application integrated using GO-Trust hardware and software technology.



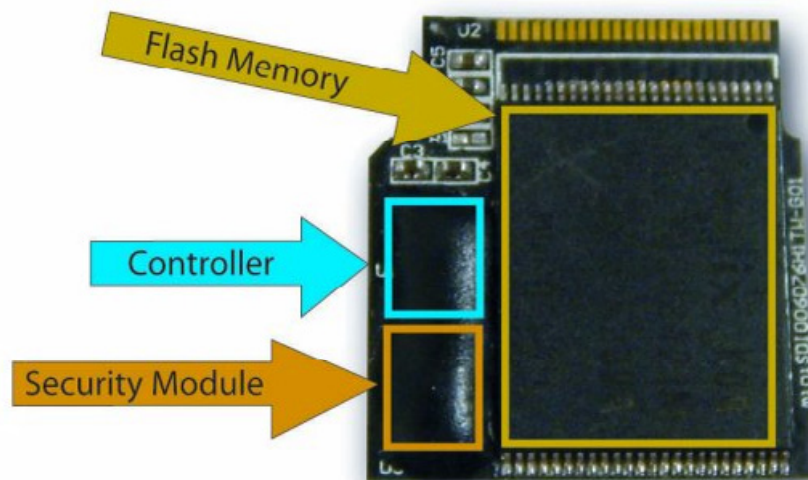


The schematic above shows how the components fit together. In a conventional SD memory card there is read/write Flash Memory and a Flash Memory Controller. In the GO-Trust SD Solution memory card the flash memory controller is replaced by a combined security module and flash memory controller. The flash memory is partitioned into standard read/write memory and protected read only memory, that contains the GO-Trust Firmware and Security library and the Developer's Application. A new module in the SD card is the security module, which I have talked about being a smart card chip, but it could also be a Java card chip or a propriety security IC. There is no new hardware in the mobile device. The security library and application are loaded from the flash memory, even auto-installed if that is supported by the mobile device.

The security application makes the same library calls it always did to the CSP, PKCS#11 or even a proprietary library. The GO-Trust library converts these calls to mass storage driver protocol, which the mobile device's operating system and mass storage driver transfer to the SD memory card. The GO-Trust SD controller separates security module commands and flash memory commands. The former are reformatted into conventional security device commands. The latter are treated as standard flash memory commands.

It is now possible to add hardware based security applications to almost any mobile device (or even office devices) that has any size of SD memory slot, even a micro SD slot. No changes are required to the mobile unit whatsoever, it will work as soon as it is unpacked from its original box. Currently available applications can easily be migrated without redevelopment and the application's delivery media (the flash memory) is included in the solution. Users plug and go, they don't have to transfer from central service providers or from a CD via their PCs. And best of all this is a NOW technology fully developed and ready to ship with your chosen security chip and application.

We looked at the GO-Trust SD Solution schematically now lets look at it physically. Not much space but it all fits in. This is an SD mini, the SD micro is an even tighter fit!



Different sizes of SD memory modules require different security chip form factors. The smallest the SD micro requires a diced wafer. The SD mini can use either a diced wafer or a Quad Flat, the very basic encapsulated diced wafer. The Standard SD module can use either of the former or a smart card module (without the external connectors).

GO-Trust SD Solution is an enabling technology so developers and manufacturers of security applications and smart cards can have security enabled SD modules with their chosen security chip and security module Operating System (COS-Card Operating System). We endeavor to make any required combination available. There are numerous opportunities created by adding robust hardware based security to mobile devices, highlighting just a few: On line transactions with strong authentication and non-repudiation, decoding streaming encrypted TV, scrambled and secure telephone calls and text messages, secure and encrypted local data vaults containing sensitive information like health records, the list goes on and on; and many of these applications are already developed elsewhere, they are just not deployed on mobile devices. Now there is nothing to stop this 'On the GO' deployment of highly secure applications on cell phones and PDAs.

