The Broad Reach of Biometrics:
Fingerprint Recognition and Mobile Security

A Farpoint Group White Paper

Document FPG 2008-435.1
November 2008

Farpoint Group believes that fingerprint scanners are poised to become the preferred – *if not dominant* – means of user authentication on highly-mobile computing and communications devices, most notably wireless handsets. All of the elements required are present today, from market and application demand to cost-effective hardware and software solutions. And we believe that the surprising degree of flexibility and suitability to many different applications inherent in this approach, coupled with the necessary reliability, convenience, and ease-of-use already present in today's implementations, will lead to a rapidly-expanding presence of fingerprint-recognition scanners across the mobile landscape.

No matter what the IT application, the requirement for strong, reliable authentication and encryption has reached the forefront of the information and network security debate. Authentication, of course, is the user proving his or her identity to the network and information resources hosted thereon, and, along with encryption, authorization (tying individual users to specific capabilities allowed) and accounting, forms the backbone of an effective network and information security strategy. But IT security solutions must be reliable without being expensive or complex, and thus the debate about how best to implement the authentication function, especially on mobile devices.

Farpoint Group has long advocated the use of *two-factor authentication* in essentially all enterprise (and certainly government) settings without regard to the size of the organization. We'd also suggest, even for consumer applications, that two-factor authentication is about to emerge as a core requirement across the board – *it's that important*. By way of definition, two-factor authentication is best described as "something you have plus something you know", thus the two factors. The "something you know" is most commonly a password or personal identity number (PIN code). Properly chosen so as to be non-obvious, and thus otherwise unrelated to a specific user and not subject to a dictionary attack (literally, attempting to break the secured system with words from a dictionary), passwords are a good start and will likely be with us for some time. To this point, the "something you have" has usually been a hardware token of some form, perhaps a smart card, synchronized password generator, or USB key. But, as we shall explore below, the "something you have" is not commonly found in most security solutions, because these items have traditionally been expensive and the resulting solution often complex.

Hence an obvious drawback with two-factor solutions: they involve an additional component which may have significant associated expense, may be inconvenient to use, and which is subject to loss, damage, theft (and consequential misuse), and failure, all usually at the worst possible time. This state of affairs has motivated the use of *biometric* security solutions, or *something you are*, literally using unique features of the user's body as the second factor. These have taken the form of facial recognition, using the built-in camera in many mobile computers and other subscriber units today, and exotic (and expensive) solutions like retinal scanners. As we will discuss below, *bioidentity* is, we believe, the key to secure mobile computing and communications going forward. But minimizing cost, complexity, and potential inconvenience must be paramount in any solution that is to have any likelihood of wide adoption and thus market success.

By far the most promising of any biometric technique is the use of a contemporary approach to a relatively ancient technology – *fingerprint recognition*. Dating to prehistoric times, fingerprints have been used for authentication and identification purposes, most commonly in criminal matters. Modern computer-based recognition techniques can have a false accept rate (FAR) of as low as .001%, and a false reject rate (FRR) of as low as .5%, meaning that it is very, very unlikely that two people attempting to authenticate through modern fingerprint recognition technology (especially using the same scanner) will be identified as the same person or that an authorized user will be locked out due to problems with a specific fingerprint scan. With the significant reductions in cost-to-solution seen in recent years, enabling installation in cell phones and similar devices, fingerprint recognition will become, we believe, the preemi-

nent solution to network and information access and security challenges - particularly in mobile environments - going forward.

Fingerprint Recognition: The Ideal Solution

The science of fingerprint recognition is based on the pattern of “hills” (or “ridges”) and “valleys” on the ventral surface of each finger, which can be examined under an optical magnifier and captured with an appropriate scanner. These patterns can be grouped into broad categories that are known as “arches”, “loops”, and “whorls”, along with other elements and any anomalies unique to a given individual. Most important are fine features known as *minutiae*. These are generally locations where a given ridge suddenly ends, or bifurcates into two ridges. Minutiae hold the key to accurate fingerprint recognition (see the Sidebar, *Fingerprint Recognition: Technology and Implementation for Mobile Phones*) and have been broadly applied in many different technical solutions. Regardless of the specific recognition strategy used, accuracy is no longer the challenge it once was in automated fingerprint recognition systems given the remarkable image quality of the small and inexpensive electronic scanners available today for this application.

Fingers, of course, have been a critical (and today familiar) element in user interface strategies and implementations for most of the history of information technology. We have, to begin, the familiar keyboard and mouse or other pointing device, as well as touch screens of various forms, which have been popular in many applications for more than 30 years. User interfaces on *mobile* devices, however, are a bit more challenging because of the limited amount of physical real estate available for the required components. Touch in a number of forms is already heavily applied in many mobile devices and applications available today, most notably in terms of the keypads and micro-keyboards (both physical and display-based) which are today practically ubiquitous as input devices on smartphones and PDA-form-factor products. Similarly, touch is the primary navigational metaphor, again via common techniques like five-way cursor keys, touch screens, stylus (pen) implementations, and gesture-based input as has been recently popularized by Apple’s iPhone. We are even today seeing some mobile products using force feedback (known as *haptics*) now becoming available, adding another dimension to the power and appeal of touch controls. In fact, Farpoint Group believes that touch-based input, navigation, and, as we will explore further below, security, will become *essential* in mobile devices going forward. We believe that the only other possible alternatives, sound and speech recognition and/or synthesis, are unlikely to become popular due to continual problems with the accuracy of speech recognition (limited vocabularies, errors resulting from noisy environments, etc.) and the fact that audio can be disturbing to others nearby - to say nothing of the potential for the compromise of sensitive information.

What we believe will allow fingerprint recognition to become a common element in mobile devices is, in fact, the long history of touch-based capabilities already discussed, combined with the low cost and high accuracy of today’s mobile solutions and the very natural intersection of an ever-increasing need for security coupled with an ever-present demand for user convenience. The latter is often why password-based single-factor authentication implementations fail; users choose passwords which are too-easily guessed by the unauthorized, or too-easily forgotten by

everyone else. Fingerprints as the second factor thus provide convenience with no compromise in overall network and information security, and fit nicely into consumer-oriented devices with minimal (if any) training and support requirements. Note, by the way, that the first factor in a two-factor solution can be a particular mobile device itself – meaning, as we'll see below, that passwords can now (securely, of course) be stored and unleashed on the fly at a user's direction with a simple swipe of a fingertip.

Given their uniqueness to a given individual, the fact that we always have (in most cases) ten of them with us at all times, and the reality that the required recognition technology is now small (including the required software footprint) cheap, accurate, simple, power-efficient, and flexible enough for even mobile-device applications, we believe that fingerprints will rapidly emerge as the *ideal* solution to the mobile authentication challenge.

Two final points: First, standards (always desirable in IT) for fingerprint recognition exist and have been broadly adopted; these are important for interoperability among applications using scanned data. Key standards include ISO/IEC 19794-2 (Information technology – Biometric data interchange formats, Part 2: Finger minutiae data), Federal Information Processing Standard (FIPS) 201, Personal Identity Verification of Federal Employees and Contractors, and ANSI INCITS 378-2004 (Information technology - Finger Minutiae Format for Data Interchange). These standards have been broadly adopted and proven secure by governments and international law enforcement agencies around the world. Not all products available today have adopted these standards, however, and a high degree of caution would as always be advised in considering non-standard implementations.

And second, Farpoint Group and others close to the technology and its applications expect the market for fingerprint recognition implementations in mobile devices to skyrocket in coming years. Fingerprint sensors in laptops are already becoming popular: market researcher Frost and Sullivan estimates that 20% of notebook computers shipped in 2008 will have integral fingerprint sensors. The potential market for cellular handsets is much larger - on the order of *one billion* units are shipped every year. Assuming just 5% of this market adopting fingerprint technology would result in 50 million units alone. Market researcher the Kerton Group, in their 2008 research brief *Market Trends for Fingerprint Sensors in Mobile Handsets*, reports a representative of Nokia stating that 10% of Nokia's phones could ship with fingerprint capability within 2-3 years, assuming fingerprint solutions achieve Nokia's desired price point. The Kerton Group further expects that eight million cell phones will ship with fingerprint scanners in 2008, and states that 43 distinct phone models have launched with fingerprint scanners since the beginning of 2007.

Fingerprint Recognition and Mobile Security Applications

Historically, of course, fingerprint recognition is best known in government-class identification applications (such as security clearances and military IDs), and, of course, for their long history of application in crime labs and other forensic settings. The technology has also been successfully applied in physical security (building access) and time-and-attendance applications as well. But with today's availability of small, cost-effective, and reliable implementations of fin-

gerprint readers and the associated software and APIs, fingerprint recognition could become, as we noted above, the most common and even standard vehicle for identification, authentication, security, authorization, and access in mobile devices going forward.

Consider just a few examples of the use of fingerprint sensors in mobile applications, as follows (see Figure 1):

- *Device access* – The most obvious application for fingerprint recognition in a mobile device is to authenticate the user and consequently allow access to the device itself. "Obvious", however, might not be the right description of this application, as most people do not lock their handsets when not in use. A stolen or lost handset can, sadly, thus become an invitation to unauthorized usage charges as well as unauthorized access to potentially sensitive information stored on the device. It has been widely reported that tens of thousands of cell phones and other handhelds devices are left in the back of taxis in just the city of Chicago every year. Farpoint Group, then, always recommends that *all* mobile computing and communications devices be secured so that only an authorized user has access. But such authorization on a handset, for example, is often limited to a personal identification number (PIN) code, which is rarely used due to the inherent inconvenience here, and which is often easily compromised. Using a fingerprint-secured device thus increases the likelihood that the user will actually lock the device (or that it will automatically lock with subsequent simple unlocking) and makes it very difficult for the unauthorized to gain access.

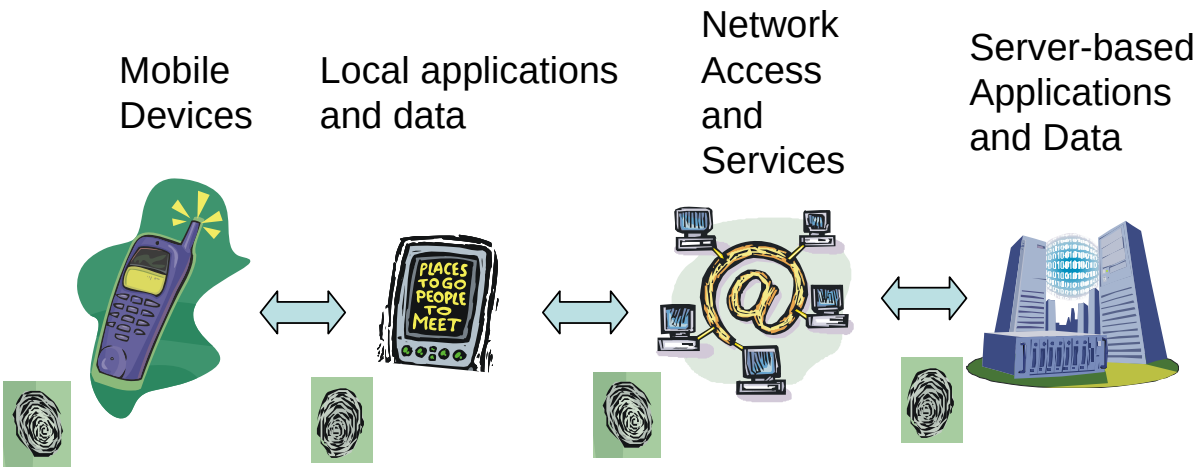

Figure 1: Fingerprint recognition can be used to authenticate, encrypt/decrypt, and otherwise unlock access to all elements of the mobile network value chain. Note that various combinations of fingerprints and ordering can be used to implement a wide variety of authentication and access possibilities. *Source:* Farpoint Group.

Note that Farpoint Group believes that this lack of mobile device security, even while widely publicized, has been and continues to be exploited with untold damage to corporations and individuals. The widespread use of BlackBerrys and other smartphones

Fingerprint Recognition: Technology and Implementation for Mobile Phones

Fingerprint recognition has come a long way from the days of crime-lab examiners using hand-held magnifying glasses to explore smudged prints lifted under field conditions. Solid-state capacitive CMOS sensors found in many laptops today provide a high degree of accuracy, with the bulk of the recognition process done by matching algorithms coded into hardware or specialized embedded software. Algorithms in the processing chain (see Figure 2) examine fingerprint minutiae, which contain the details specific to a given individual. Industry standards specify fingerprint minutia file formats so that fingerprint components and solutions can properly interoperate.

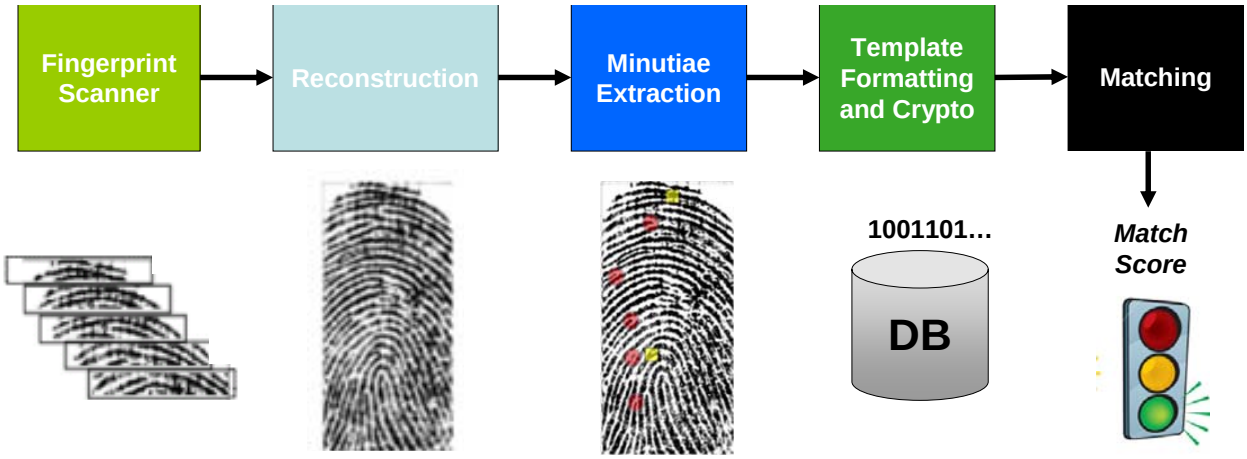

Figure 2: While fingerprint recognition can be technically complex, the required processing can today be easily embedded in VLSI-based implementations. The algorithms and data required also have a small computational footprint, simplifying handset-based designs. *Source:* Atrua Technologies.

Features required for a fingerprint product well-suited to mobile handsets include:

- *Accuracy* – The implementation should be able to achieve a false acceptance rate of 0.01% or lower, and work in a broad range of devices and environments.
- *Security* – All biometric information and other private information stored in the phone's memory must be protected from unauthorized access. Integration with SIM cards and other handset security features is desirable.
- *Low power consumption* – Low current consumption in both standby and active imaging modes is required in order to minimize drain on the always-limited battery charge.
- *Small form factor* – There isn't much space available on a handset, so sensor real estate must be minimized. Scanners (reading the swipe of a finger) are therefore the preferred approach here.
- *Highly integrated* – Effective designs require only a small number of external components to assure that solution cost and physical size are minimal.

- *Efficient use of platform resources* – Fast match times are required while minimizing both processor MIPS and memory footprint.

- *Standards-based interface using fingerprint minutia templates* – As we noted elsewhere, standards-based interfaces provide a design and operational flexibility. ISO 19794-2 templates can be stored on a SIM or other secure element and moved from one fingerprint phone to another.

- *Navigation and convenience features* – A real plus in terms of both cost and physical real estate is for the fingerprint sensor to additionally act as a touch input device, providing the ability to navigate a user interface or access favorite destinations without typing. Haptic feedback is also desirable in highly-mobile devices, and we believe such will become very popular as display-optimizing touch user interfaces grow in popularity

"Integrating fingerprint recognition into mobile devices is a relatively straightforward task," said Carl Temme, VP of Marketing at fingerprint-recognition component manufacturer Atrua Technologies, in an interview. "Only one, low-cost, active component is required. We provide all the embedded code required for the mobile device including the signal-processing algorithms, standards-based minutia interfaces, the common API for applications, and secure management of scanned data. And solutions are extremely cost-effective".

A block diagram and illustration of the principle of operation for Atrua's ATW300 Made-For-Mobile™ fingerprint sensor is shown in Figure 3. Note that the specifications of this device include optimization for a battery powered environment - standby power is only 2.6 uA, and the power required for active imaging (scanning) is only 1.4 mA.

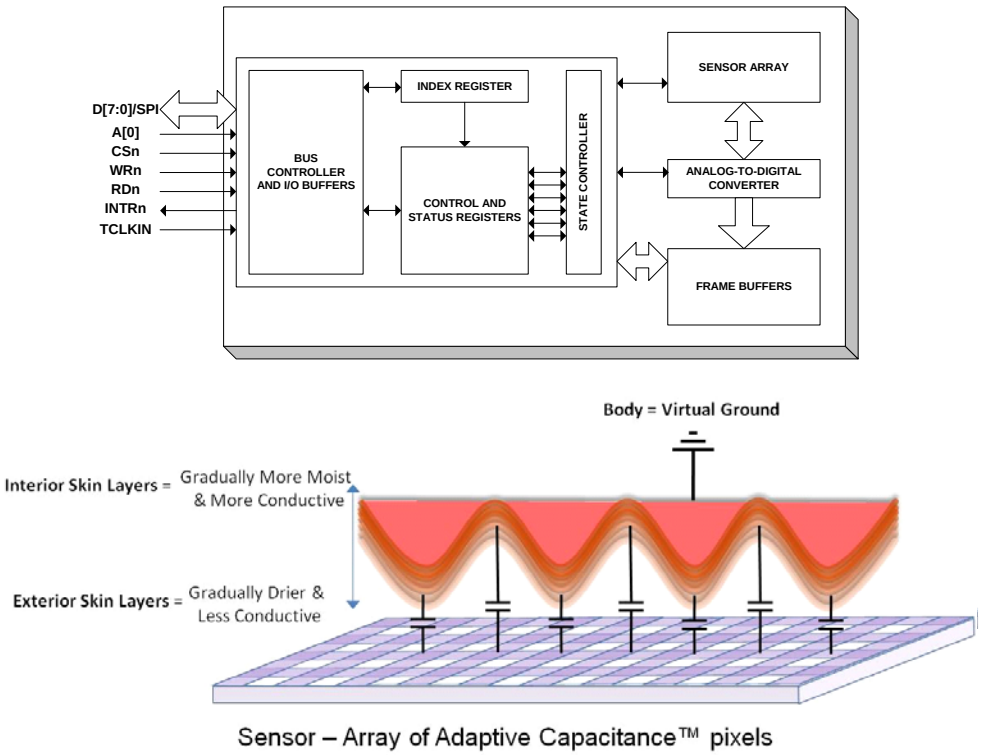

Figure 3: Implementation of fingerprint recognition hardware is relatively simple, thanks to robust VLSI-based vendor implementations and simple capacitive scanners. Interfacing requirements are on the order of those required for typical I/O devices. *Source:* Atrua Technologies.

which hold or have access to sensitive corporate and personal data contained in e-mails, documents, and spreadsheets has created an easy portal for criminals, including professional information and identity thieves. Some companies wisely implement mobile-device-management remote-lock/wipe (or "zap") features to protect data, but there can often be a substantial delay before a user recognizes that their device is missing and this action is taken. Even then, the protection provided by remote lock/wipe is easily circumvented if the thief removes the battery or shields the device from wireless signals.

- *Information access* – Once one has access to the device, the next issue is securing any sensitive data stored on it. One might argue that the use of fingerprint-recognition technology for access to the device is enough, but this ignores the possibility that sensitive data might be stored on a removable memory card, or that a dedicated information thief might even disassemble the device and extract any FLASH memory chips or other storage medium. Farpoint Group thus recommends that *any* sensitive (as defined by a local security policy) data stored on *any* mobile device be encrypted and made available *only* to an authorized user and then *only* upon the authentication of that user. Just as fingerprint recognition can provide authentication, it can also be used as a basis for the generation of or access to encryption keys. It would be incredibly difficult for anyone to work around such a protection mechanism, which is obviously much more challenging than guessing a pin code or finding same via exhaustive search or a dictionary attack.

- *Network access* – Similarly, fingerprint-recognition data can be used to provide identification information for logging into a network, and can also serve as a key element in generating or accessing an encryption key or a one-time-password required for a virtual private network (VPN) or similar network-security scheme. The embedding of fingerprint recognition capability in a mobile device eliminates the need for a separate password/key generator, such as those that are frequently implemented as small hardware devices with a simple LCD display and synchronized with the target system. There is, after all, little chance a fingerprint can be stolen or otherwise compromised – and fingerprints are not expensive, will not suffer from dead batteries, and cannot be lost. And, of course, given ten different fingerprints, users can apply different fingers to initiate access to different networks or services easily, efficiently, and accurately.

- *Service/application authorization and access* – Finally, fingerprint recognition can be used to authorize access to specific network services or applications, leaving little doubt that a user is who they claim to be and that they are in fact authorized (via RADIUS or a similar mechanism) to be initiating the services that they request.

So, in summary, a fingerprint reader installed in a mobile handset or similar device can be used as the primary vehicle for authorizing access to the device itself, encrypting data stored on the device or on a network to which it connects, authorizing access to secured or encrypted data and allowing access to any security keys required for decryption and access, gaining access to a given network, and authorizing access to services and applications on the network – essentially *every* security-related activity required by enterprise users. But consider also these common consumer-class applications, using exactly the same technologies:

- *M-Commerce* – Farpoint Group believes that mobile e-commerce, or *m-commerce*, will be a key driver of the wireless industry for some time to come. Loosely defined, m-commerce is the ability to buy products and services using a mobile device anywhere access to a supported network is available, and is applicable in both pure-consumer and business-to-business settings. Most m-commerce transactions involve a credit or debit card, which itself is less than secure, but even more vulnerable to theft and error when the user has to enter a credit card number and supporting information on a mobile device. A fingerprint could be used here as the key to a secured file containing credit card information, with applications assuring that the card information itself never appears in the clear and is always sent over a secured connection – secured, again, with a fingerprint. In addition to the security advantage, this approach eliminates the inconvenience of digging out a card and manually entering a credit card number using a mobile keypad, a major barrier for those of us with limited patience and (especially) time.

  Note also that m-commerce transactions will increasingly involve the use of wireless technologies other than cellular and even Wi-Fi connections, with nearfield communications (NFC) and related contactless short-range technologies becoming, we believe, very popular. But wireless credit card readers based on *any* radio technology introduce the potential for financial data to be stolen while in transit through the air, and thus motivate the need for appropriate security solutions. A fingerprint can be used to secure these links in a manner identical to any other communications or networking application. In a first-of-its-kind trial conducted in the United States by Cellular South, Bank of America, and MasterCard, the security and convenience of fingerprint was taken further, providing users the ability to open their "electronic wallet" across a secured NFC link and select their preferred payment card all with the swipe of their designated "payment finger".

- *Other financial transactions* – This model can be extended to all forms of financial transactions beyond those using credit cards, including banking, brokerage, and related types of services. We believe it is likely that financial institutions will insist on some form of two-factor authentication in the future to reduce the cost of fraud, with fingerprint recognition being the simple and convenient solution. Convenience that encourages transactions is a key element in financial services today and clearly driving such initiatives as MasterCard's PayPass and Visa's payWave contactless payment systems. Adding fingerprint recognition here is a simple and natural improvement beyond basic capability.

- *Digital signatures* – A fingerprint is an ideal digital signature, extremely difficult to forge and with natural duplicates existing only very, very rarely. We thus have a simple and reliable mechanism to authenticate identity and establish authenticity of and ownership for documents and transactions.

- *Combined solutions* – Note that a fingerprint can be used in conjunction with a SIM card or similar hardware token to implement a complete two-factor authentication solution. When combined with a PIN code or password, creating a three-factor (and yet still very convenient and easy-to-use) solution, the resulting combination is as secure as

could be expected in the commercial world. Adding in government-grade security, such as compliance with the FIPS 140-2 specification, one could imagine no better security solution - on par with those used in military and national-security applications.

We thus believe that fingerprint sensors (and, we might add, related touch-based navigational devices) will become key user interface metaphors for many - *if not most* - future mobile devices. Fingerprint recognition can be also used to enter commands into mobile and Web-based applications, simplifying interaction via what might otherwise be a complex sequence of commands. When combined with haptics, we may in fact find that fingerprints are the key to truly efficient - *if not ideal* - mobile user interfaces in the very near future.

Conclusion – The Ideal Solution

As we have shown in this White Paper, fingerprint recognition technology is likely to become the methodology of choice for *all* aspects of mobile security across a broad range of applications and usage scenarios. The technology can be implemented in essentially all handsets and related mobile devices, and has the right combination of security, cost, and convenience for the user. It is well-suited to the authentication, authorization, and encryption required for the device, file, and transactional security requirements of modern applications. It may very well be that the mainstream technologies of wallets and pocketbooks are finally headed for the scrapheap, with something that has been with us even longer - the fingerprint - taking their place.

Fingerprint recognition is now available on a number of mobile devices, including the beautiful and elegant Porsche P'9521 (built by Sagem; see Figure 4) handset and Windows Mobile devices including the Toshiba G910, G900 and G500. But, no matter the specific mobile PC or handset, fingerprint recognition yields the single personal identifier that can work with every element of an IT solution, from the handset to the PC, the network, servers, applications, and whatever else might be required - today or tomorrow.

Figure 4: Mobile handset (the Porsche P'9521) equipped with fingerprint sensor (at bottom of screen). *Source:* Atrua Technologies.

Ashland MA 01721
508-881-6467
www.farpointgroup.com
info@farpointgroup.com

The information and analysis contained in this document are based upon publicly-available information sources and are believed to be correct as of the date of publication. Farpoint Group assumes no liability for any inaccuracies which may be present herein. Revisions to this document may be issued, without notice, from time to time.

Copyright 2008 — All rights reserved

Permission to reproduce and distribute this document is granted provided this copyright notice is included and no modifications are made to the original.