Position Paper ■

Wireless Technology Infrastructures for Authentication of Patients: PKI that Rings

Ulrich Sax, PhD, Isaac Kohane, MD, PhD, Kenneth D. Mandl, MD, MPH

Abstract As the public interest in consumer-driven electronic health care applications rises, so do concerns about the privacy and security of these applications. Achieving a balance between providing the necessary security while promoting user acceptance is a major obstacle in large-scale deployment of applications such as personal health records (PHRs). Robust and reliable forms of authentication are needed for PHRs, as the record will often contain sensitive and protected health information, including the patient's own annotations. Since the health care industry per se is unlikely to succeed at single-handedly developing and deploying a large scale, national authentication infrastructure, it makes sense to leverage existing hardware, software, and networks. This report proposes a new model for authentication of users to health care information applications, leveraging wireless mobile devices. Cell phones are widely distributed, have high user acceptance, and offer advanced security protocols.
The authors propose harnessing this technology for the strong authentication of individuals by creating a registration authority and an authentication service, and examine the problems and promise of such a system.

■ **J Am Med Inform Assoc.** 2005;12:263–268. DOI 10.1197/jamia.M1681.

More than seven years after the National Academy of Sciences and the National Research Council called for more stringent authentication measures for access to electronic medical records,[1] most medical applications still rely on simple username and password for identification and authentication of the patient.[2–10] More advanced authentication methods, such as public key encryption, have failed to gain a foothold, never achieving user acceptance, nor spawning the massive infrastructure required. Implementing increasingly secure approaches will be particularly challenging for the evolving suite of consumer health applications, since the technology must be accessible even to citizens with very limited experience using computers. The efforts to develop a robust infrastructure for consumer-driven health applications, such as personally controlled health records,[5–16] in the absence of a universal health care identifier[17,18] bring the problem of authentication to the forefront of challenges in medical informatics.

Conventional wisdom dictates that secure authentication requires the user to meet at least two of the following criteria: to present something she knows, something indicating where she is located, something related to who she is, or something she carries.[4] An increasing portion of the population carries wireless mobile devices, mostly cellular telephones.[19,20] Access to this rapidly advancing equipment cuts a broad swath across the socioeconomic spectrum.[21] Cell phones are currently in use in several health care projects and are being used for data display and even basic authentication.[22–25]

Cell phone technology represents a potentially viable way of solving the authentication problem at local, regional, and national levels. This report proposes a new model for authentication of users to health care information applications leveraging wireless mobile devices and critically examines its problems and promise.

State of the Art Authentication Methods

Authentication is the identification of a person or machine and the subsequent verification of that identity claim. The first generation of consumer health applications, including personally controlled health records, rely solely on username and password, the most basic and least secure method to verify a claim of identity.[5–10,14,26] Protocols for assigning and maintaining user names (identifying a user to the system) and passwords (a shared secret to verify the identity of the user) are standard. Consumers familiar with a host of non–health care–related websites readily understand their use. Passwords, however, can be easily compromised, using social engineering[27] or simple attack methods such as key loggers and password crackers.[28,29]

Strong authentication, on the other hand, enables users to provide evidence that they know a particular secret without actually revealing that secret.[30] The most well known strong authentication system is pubic key encryption and the related public key infrastructure (PKI).[31] PKI provides a method to ensure that the sender can encrypt a message, which the receiver can decrypt, while preventing anyone who intercepts

Affiliations of the authors: Children's Hospital Informatics Program (US, IK, KDM) and Division of Emergency Medicine, Children's Hospital Boston, (IK, KDM); Harvard Medical School, (US, IK, KDM) Boston, MA.

This work was supported by Deutsche Forschungsgemeinschaft (DFG, SA1009/1-1) and by the National Institutes of Health through contract N01-LM-3-3515 from the National Library of Medicine.

The authors thank Bill Simons, Pete Szolovits, Matvey B. Palchuk, Teresa Zayas-Cabán, Min Wu, and Peter Pharow for their input.

Correspondence and reprints: Ulrich Sax, PhD, Children's Hospital Informatics Program, 1 Autumn Street AU543, Boston, MA 02115; e-mail: <usax@med.uni-goettingen.de>.

Received for publication: 08/20/04; accepted for publication: 12/20/04.

the message from reading it.[32] The sender and receiver get a pair of public and private keys. These keys are mathematically related. To encrypt a message for a certain receiver, the sender uses the receiver's public key for encryption. Only the intended receiver can decrypt this message with his private key. PKI requires a certification authority for issuing digital certificates, a registration authority maintaining the records of the PKI users in a directory service, a policy framework governing certificate issuance and cancellation, and PKI-enabled applications.

It was long assumed that PKI would be widely adopted; however, to date, the technology has proven expensive and too complex for information technology (IT) professionals and end users.[33–37] Several electronic health record projects encountered substantial difficulties implementing PKI, the most challenging being key distribution and end user support.[33,38] The 2002 Medical Records Institute Status Report on Electronic Health Records in the United States[10] found only 10% of the respondents using public key encryption for health record authentication.

Another approach to authentication is biometrics, identifying individuals by their anthropometric characteristics as measured by fingerprint, iris, or retinal scan; facial recognition; patterns of speech; keyboard strokes; or handwriting dynamics.[39] Evaluating the output of a typical biometric device is much more complex and has much higher failure rates than simple username password schemes.[40] In addition, a concern with biometric methods is that individual characteristics cannot be revoked or changed if compromised, as we have a limited number of biometric characteristics. It has been shown that many biometric methods, especially fingerprint recognition, are highly susceptible to security breaches.[41]

The use of biometrics in medical record authentication is rare. Only 2.4% of the responders to the 2002 Medical Records Institute survey used biometrics for health record authentication.[10] A major problem with the use of biometrics in consumer applications is that, as with the use of smart cards—a failed approach for health care applications in the United States[37,42] —the system necessarily relies on wide distribution, support, and maintenance of hardware.

Wireless Authentication Infrastructure

Since the health care industry is unlikely to spawn and maintain a distinct, hardware-based authentication infrastructure, it makes sense for health care applications to rely on existing hardware, software, and networks. PKI implementations, to date, have failed in the United States, but the technology may be resuscitated if piggybacked on a successful existing infrastructure. At least 62% of all adults owned a mobile phone in 2001[43,44] and by 2003, 66% of all U.S. households owned mobile phones.[21,43] As with all costly technologies, there looms the concern of a digital divide. Low-income families are more likely to have no or suboptimal cell phones.[43–45] However, even among families of underrepresented minorities, the penetration rate of this technology is high.[20,21]

In the United States, four incompatible cellular phone systems compete for market share. Of these, the Global System for Mobile Communications (GSM) and General Packet Radio Service (GPRS) offer authentication capabilities, using a built-in Subscriber Identity Module (SIM) card to store a secret key. The GSM or GPRS currently covers only 11% of U.S. cell phone subscribers but is trending upwards.[46] Third-generation (3G) cellular equipment with much faster connections and the Universal SIM (USIM) card will likely gain a large share of the market in the near future.[47] The 3G cell phone system was developed by a worldwide consortium and is accepted internationally. Many U.S. cell phone providers plan to upgrade from their respective technologies toward 3G.[48]

Form Factors of PKI-Related Devices

PKI-related information, such as keys and key certificates, may be stored on different devices, each with advantages and disadvantages. In Table 1 we compare features across various methods for distribution of PKI certificates and keys. Each form factor contains a cryptographic key and a corresponding key certificate. In the first case, key files on a computer, these files are stored directly on a hard or floppy disk. Cryptographic hardware stores and protects these files in a dedicated electronic circuit. Smartcards as well as USB tokens store the files on a standardized chip,[49–51] which can be interfaced with a computer. There are a variety of smartcards in use. Storage cards, including some older European health insurance cards, can be copied easily; protected storage cards like prepaid telephone cards cannot be copied. Smartcards with a cryptographic coprocessor offering PKI functionality are commonly deployed in cell phones.

In Table 2 we give an overview of four different approaches for wireless authentication. SIM cards in wireless equipment are well standardized.[52] Cell phone providers use them to store items such as the name of the service provider, International Mobile Subscriber Identity (IMSI), ciphering key, and the user's preferred language and telephone numbers.

An advantage of these plug in cards is that they do not need a dedicated interface to a computer because the card reader is built in. Although already in use for financial transactions, for example at European gas stations,[53] SIM authentication is not secure. The key length is insufficient,[54,55] and the encryption can be defeated.[56] Next-generation 3G phones with USIM remedy these shortcomings and offer high security.[57,58] USIM-equipped mobile phones hold substantial promise in terms of security, functionality, usability, portability, and cost.

The rapidly evolving wireless market, which promises ubiquity of these devices, provides an attractive option for the backbone of a health care application authentication infrastructure. A universal health care authentication mechanism relying on these technologies necessitates a staged approach to implementation, accounting for current and future capabilities. To motivate our proposal and serve as a basis for our analysis, we present a usage scenario:

> Helen arrives at an emergency department and wishes to authorize access to her personally controlled health record.[14,59] She uses her cell phone to call the toll free number of an authentication service. A challenge message is sent to her handset. The handset decrypts the message and encrypts it again with the private key stored in the USIM. To enable the USIM to re-encrypt the message, Helen is prompted to key in a personal identification number, which she has chosen and committed to memory. Helen is then prompted to key in the hospital ID number prominently displayed over the triage desk. Responding in the affirmative, the authentication service contacts the PHR, Helen's record appears on the registration

Table 1 ■ Assessment of Several Form Factors of PKI-Related Devices

	Form Factor of PKI Device					
	Key-file/PC*	Crypto Hardware/PC§	Smart Card/PC	USB Token/PC	Mobile Equipment with SIM	Mobile Equipment with USIM
Security	Low†	High	High	High	Moderate	High
Functionality	High	High	High	Moderate#	High	High
Usability	High	Low‖	Low¶	Moderate#	High	High
Portability	Moderate‡	Low	Moderate¶	Moderate**	High	High
Ubiquity	High	Low	Moderate	High	Moderate††	Low§§
Cost	Low	Moderate	High	Moderate	Low	Low
PKI ability	Moderate	Moderate	High	High	Low‡‡	High

*The cryptographic key is not stored on a device like a Smart Card, but in a simple ASCII file.
†A key file can be copied or deleted.
‡Portable if on external storage media, needs PKI client software.
§A device like a computer plug in card containing a crypto processor.
‖Limited to use with a single computer from a particular vendor.
¶Card reader and driver needed.
#No card reader needed (USB port) but additional driver needed.
**Still driver needed, additional device to handle.
††Almost 2/3 of all US adults own a cell phone, GSM phones currently have a 11% market share.
‡‡Due to short key length and cracked cryptographic algorithms the SIM chip is not adequate for secure authentication.
§§First 3G phones are available now in Europe and Japan, but do not have market penetration in the US yet.

Table 2 ■ Assessment of Approaches for Wireless Authentication

	Approach for Wireless Authentication			
	Mobile Equipment without SIM	Mobile Equipment with WIM	Mobile Equipment with SIM	Mobile Equipment with USIM
Wireless communications standard	All systems	WAP2.0 enabled	GSM, GPRS, EDGE	3G
Number of keys	1 **symmetric**	1 **asymmetric** pair	1 **symmetric**	2 symmetric, Many **asymmetric** pairs
Key length	n/a*	Variable	32 bit	128 bit symmetric, no length limit for asymmetric
Key storage	n/a	WIM, USIM	SIM	USIM, WIM
Mechanism	RSA challenge via SMS	Wireless Transport Layer Security (WTLS)	Cell phone authentication with shared key	Mutual authentication, PKI
Authentication strength	Moderate†	Strong	Weak‡	Strong

*Symmetric key combined with world time called "passcode."
†Broadly used in VPN environments.
‡Short key length and compromised, not published algorithm; no authentication of the base station.

screen in the emergency department, and hospital staff is granted web access to portions of the record, set according to Helen's pre-specified preferences.

Trust

The first task in establishing a wireless authentication infrastructure—a critical one—is to establish the necessary web of trust for reliably linking each citizen with a mobile device. The existing infrastructure used by telecoms to establish mobile service contracts only partially accomplishes this objective. Mobile subscribers generally are authenticated at the time of enrollment by passport or driver's license and social security number. The information used by telecoms to link citizens to mobile devices is not currently available to the health care system, although future telecom business models may be built around providing such services.[23,24]

Toward the end of establishing a patient's identity and linking that patient to a piece of equipment, it seems most reasonable to leverage the existing trust relationships that underlie current health care information exchange. The root of trust in health care is and always has been the patient–physician relationship. Patients are known to their primary care and specialty practices; identification of patients is best accomplished in this setting. We are not suggesting that physicians become notaries. Rather, we observe that the existing web of trust upon which the health care system relies tends to preclude the sort of wholesale large-scale fraud that might occur in a system that closes the loop without this human–human interaction required for every new registrant. Hence, we envision patients "signing up" and entering the system in private clinic-based and hospital-based physician offices.

Cryptographic Authentication

The linkage established at a physician's office must be uploaded to a mobile authentication service, which provides a directory service including an international subscriber directory number identifying the phone subscriber and the unique serial number of the cell phone and the plugged-in USIM Chip. When the user (for example in the scenario above) is being contacted by the authentication center, her mobile equipment receives a challenge. The mobile equipment responds to the challenge, and, if successful, the mobile authentication service informs the web portal. A simple response can be made with any mobile phone. A mobile authentication service sends a Short Message Service (SMS) message to the user's phone, which, in turn, responds uniquely after the user keys in a personal identification number. Authentication here relies on the RSA algorithm (Table 2).[60]

This approach provides strong authentication because it relies on the fact that a user is in the possession of a mobile phone linked to the user as described above and that he knows the corresponding PIN. A more sophisticated response approach requires a smart phone running the Wireless Application Protocol (WAP) 2.0 and utilizes public key encryption to achieve higher security. The cryptographic keys are stored on the Wireless Identity Module (WIM).[25,61] Other approaches rely on the SIM card on GSM and GPRS networks and USIM cards on 3G networks. The encryption capabilities provided by the SIM card are limited by its storage capacity; hence, the weak authentication protocol.[55] The USIM specification[57,58] provides storage capacity for many asymmetric keys without restricting key length, thus, substantially improving the strength of authentication.

Major Challenges

Infrastructure

A secure and acceptable mobile authentication service requires advances in market penetration of 3G cell phones to perform strong authentication. The mobile authentication service has to be run and funded by a trustworthy party because it forms the backbone of trust. Although the mobile communications infrastructure enables a high level of authentication, significant additional investments are required to adapt these technologies for health care needs. Direct costs to support the functionality of the above scenario include improvements to the existing mobile messaging infrastructure beyond the initial costs of the existing authentication-enabled devices, for example, the authentication and registration services.

Furthermore, there are costs associated with issuing and maintaining certificates, and providing the necessary user support. Business models for the operation of the mobile authentication service have to be created and vetted, if "piggy-backing" on existing processes is not possible in the short term. The authentication services would likely offer the greatest return on investment if used for general consumer applications. Hence, they may be bundled with generic services by telecommunications companies or as joint ventures with commercial or governmental organizations within the health care industry.

Usability

In the course of launching PHRs and other consumer informatics applications, awareness of security risks associated with protected health care information must be raised among consumers.[39,62] There will be technical hurdles to overcome as well. For example, the lag between the log in on the portal site and the availability of the application could pose another problem. Usually it takes about 3 to 5 seconds to receive an SMS. Longer time lags caused by additional procedures would likely decrease the user acceptance.

Backups and Contingency Plans

Because patients will certainly forget to bring, change, and lose their cell phones, no single authentication method will suffice. If a patient loses a cell phone or wants to use a new cell phone (10% of cell phone subscribers in the United States plan to switch their provider within the next year[43]), the mobile authentication service profile has to be updated very quickly. Also, there are special populations to consider. Children will need to be authenticated by parents or guardians. Patients receiving emergency care may not be able to use their phones. What is needed is a multilayered access control system, allowing the user to choose the level of authentication. For weaker methods, (username and password) additional security may be obtained by adding the additional hurdle of challenge questions (e.g., place of birth, favorite color). An option would be to provide less access for lesser levels of authentication (for example, only access to problem list, medications, and allergies). Users would also have to be given the opportunity to allow emergency access to their record should they be incapacitated. Further, should the process fail because of technical problems, such as network unavailability, fallback infrastructures will need to be in place.

Conclusion

Secure authentication is a critical requirement for a new generation of consumer-driven health care applications, such as PHRs. Because mobile technology may be costly, the concern of a digital divide has to be addressed. Although wireless technology penetration is high even among families of underrepresented minorities,[22,45] low-income families are more likely to have no or suboptimal cell phones.[43,44] The major issues that need to be addressed to enable a large-scale deployment of the proposed technology are infrastructural, particularly development of a registration process, creation of a trusted mobile authentication service, and provision of user support.

To establish a robust national health information infrastructure, going forward, the health care system must develop standardized methods of authenticating patients. It seems wise to begin leveraging systems that already have wide-scale use and consumer acceptance. There are bold challenges to meet in adapting cell phone networks for this purpose, not the least of which is creating a directory linking people to their mobile equipment. The obstacles notwithstanding, wireless authentication enables use of PKI functionality while avoiding many of the problems that plagued the traditional PKI implementations; there is no need for additional tokens, card readers and drivers, or unfamiliar security procedures. It seems safe to assume that people will be routinely carrying sophisticated wireless devices with them for some time to come. The health care industry should explore this mainstream technology as a potential solution to a decades-old problem.

References ■

1. For the Record: Protecting electronic health information. In: Board CSaT, Council NR (eds). For the Record—Protecting Electronic Health Information. Washington, DC: National Academy Press, 1997.

2. HarrisInteractive. Two in five adults keep personal or family health records and almost everybody thinks this is a good idea. Harris Interactive Market Research. Available at: http://www.harrisinteractive.com/news/newsletters/healthnews/HI_HealthCareNews2004Vol4_Iss13.pdf. Accessed August 19, 2004.
3. HarrisInteractive. eHealth's influence continues to grow as usage of the internet by physicians and patients increases. Available at: http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=608. Accessed August 16, 2004.
4. HarrisInteractive. Internet penetration at 66% of adults (137 million) nationwide. The Harris Poll #18. April 17, 2002. Available at: http://www.harrisinteractive.com/harris_poll/index.asp?PID=295. Accessed August 16, 2004.
5. Riva A, Mandl KD, Oh DH, et al. The personal internetworked notary and guardian. Int J Med Inf. 2001;62:27–40.
6. (IOM) IoM. Key capabilities of an electronic health record system—Letter Report. July 31, 2003. Available at: http://books.nap.edu/html/ehr/NI000427.pdf. Accessed August 16, 2004.
7. Sittig DF. Personal health records on the internet: a snapshot of the pioneers at the end of the 20th Century. Int J Med Inf. 2002;65:1–6.
8. Kim MI, Johnson KB. Personal health records—evaluation of functionality and utility. J Am Med Inform Assoc. 2002;9:171–80.
9. Ueckert FK, Prokosch HU. Implementing security and access control mechanisms for an electronic healthcare record. Proc AMIA Symp. 2002;825–9.
10. Waegemann CP. Status report 2002: electronic health records. Boston, MA: Medical Records Institute. Available at: http://www.medrecinst.com/resources/ehr2002/index.shtml. Accessed August 16, 2004.
11. Thompson TG, Brailer JB. The decade of health information technology: delivering consumer-centric and information-rich health care: framework for strategic action. Department of Health and Human Services. Available at: http://www.hhs.gov/onchit/framework/. Accessed August 16, 2004.
12. Markle Foundation. The Personal Health Working Group Final Report. *Markle Foundation*. Available at: http://www.markle.org/downloadable_assets/final_phwg_report1.pdf. Accessed August 16, 2004.
13. Uckert F, Ataian M, Gorz M, Prokosch HU. Functions of an electronic health record. Int J Comput Dent. 2002;5:125–32.
14. Mandl KD, Szolovits P, Kohane IS. Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ. 2001;322:283–7.
15. CareGroup. PatientSite (online Personal Health Record). Available at: https://patientsite.bidmc.harvard.edu/. Accessed August 16, 2004.
16. Simons WW, Mandl KD, Kohane IS. The PING personally controlled electronic medical record system: technical architecture. J Am Med Inform Assoc. 2005;12:47–54.
17. Kohane IS, Dong H, Szolovits P. Health information identification and de-identification toolkit. Proc AMIA Symp. 1998;356–60.
18. IEEE-USA. Voluntary Healthcare Identifier. IEEE-USA, Washington DC. June 17, 2004. Available at: http://www.ieeeusa.org/policy/positions/healthcareidentifier.html. Accessed November 9, 2004.
19. Entner R. Third Quarter 2002 U.S. Wireless Forecast 2000-2006. The Yankee Group, Boston, MA. Available at: http://techupdate.zdnet.com/techupdate/stories/main/Third_Quarter_2002_US_Wireless_Forecast_2000_2006.html?tag=tu.tk.6656.f1. Accessed August 16, 2004.
20. Scarborough Research. Hispanics' cellular bills are 10% greater than the international average. Scarborough Research. Available at: http://www.scarborough.com/press_releases/Hispanic%20cell%20phone%20FINAL%20English%202.18.04.pdf. Accessed August 16, 2004.
21. Horrigan J. Consumption of information goods and services in the United States. Pew Internet & American Life. Available at: http://www.pewinternet.org/pdfs/PIP_Info_Consumption.pdf. Accessed August 16, 2004.
22. Sneiderman CA, Ackerman MJ. Cellular radio telecommunication for health care: benefits and risks. A brief review. J Am Med Inform Assoc. 2005;11:479–81.
23. Nielsen W. Mobile phones can be utilized in critical areas such as healthcare. 1st-In-Cell-Phones.com. Available at: http://www.1st-in-cell-phones.com/21908-mobile-phone-applications.html. Accessed August 16, 2004.
24. Schuerenberg BK. Will health care get smart? Mobile Health Data. Available at: http://mobilehealthdata.com/article.cfm?articleId=494&banner=b1. Accessed August 16, 2004.
25. Bielli E, Carminati F, La Capra S, Lina M, Brunelli C, Tamburini M. A wireless health outcomes monitoring system (WHOMS): development and field testing with cancer patients using mobile phones. BMC Med Inform Decis Mak. 4(1):7.
26. Personal Health Working Group. Personal Health Working Group—Final Report. Boston, MA: 2003.
27. Smith SW. Probing end-user IT security practices through homework. The EDUCAUASE Quarterly. 2004;27(4):68–71.
28. Proctor RW, Lien MC, Vu KP, Schultz EE, Salvendy G. Improving computer security for authentication of users: influence of proactive password restrictions. Behav Res Methods Instrum Comput. 2002;34(2):163–9.
29. VeriSign White paper. The security risks of using passwords. Available at: http://www.safescrypt.com/resources/PasswordWhitePaper.pdf. Accessed August 16, 2004.
30. Tardo J, Alagappan K. SPX: Global authentication using public key certificates. Proc IEEE Symp. Research in Security and Privacy. May 20-22, 1991:232–44.
31. Chousiadis C, Mavridis IK, Pangalos GI. An authentication architecture for healthcare information systems. Health Informatics Journal. 2002;2002(8):199–204.
32. Szolovits P, Kohane I. Against simple universal health-care identifiers. J Am Med Inform Assoc. 1994;1(4):316–9.
33. Blobel B, Kaliontzglou A, Bourka A, Georgoulas A. Report on scenarios demonstration and assessment of pilot operation (RESHEN). Available at: http://www.biomed.ntua.gr/reshen/Main/Project_Organisation/Current_Status/current_status.html. Accessed August 16, 2004.
34. Computer Science and Telecommunications Board. Technical challenges—security. In: Committee on Enhancing the Internet for Health Applications: Technical Requirements and Implementation Strategies. Networking Health-Prescriptions for the Internet. Washington, DC: National Acadamy Press, 2000.
35. Bourka A, Kaliontzoglou A, Polemi D, Georgoulas A, Sklavos P. PKI-based security of electronic healthcare documents. Proceedings of the SSGRR 2003R, L'Aquila, Italy, January 6-12, 2003. Available at: http://galeb.etf.bg.ac.yu/~vm/cd1/papers/118.pdf. Accessed August 16, 2004.
36. Altrogge M. Public-key-infrastructure: secure obstacles (German: Sichere Stolpersteine). Network Computing. 2003;1–2.
37. HIMSS. Annual HIMSS Leadership Survey: Final Report: Providers. HIMSS. Available at: http://www.himss.org/2002survey/final_report_07.htm. Accessed August 16, 2004.
38. Tunitas. PKI readiness evaluation. Tunitas Group. Available at: http://www.tunitas.com/pages/PKI/PKI_readiness.html. Accessed August 16, 2004.
39. ITRC. Identity theft resource center. A nonprofit organization. Available at: http://www.idtheftcenter.org/index.shtml. Accessed August 16, 2004.
40. Lassmann GE. Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren (Catalogue of Criteria for Evaluating the Comparability of Biometric Methods, German only). Teletrust Germany e.V., Erfurt, Germany. Available at: http://www.teletrust.de/down/kritkat_2-0.zip. Accessed August 16, 2004.
41. Thalheim L, Krissler J, Ziegler P-M. Body check—biometric access protection devices and their programs put to the test. c't,

Magazin für Computertechnik heise-Verlag, Hannover, Germany. Available at: http://heise.de/ct/english/02/11/114. Accessed March 11, 2005. (11/2002):114–123.

42. MeT. MeT Consistent User Experience. Mobile electronic Transactions (Ericsson, Panasonic, NEC, Nokia, Siemens et al.). Available at: http://www.mobiletransaction.org/pdf/R200/specifications/MeT_CUESpec_v200.pdf. Accessed August 16, 2004.
43. Scarborough Research. Atlanta, GA; Detroit, MI; and Austin, TX ring the loudest when it comes to cell phone ownership. Scarborough_Research. Available at: http://www.scarborough.com/press_releases/10_03_cellphone_local%20market.pdf. Accessed August 16, 2004.
44. Scarborough Research. Cell phone ownership grows 29 percent from 1999-2001 according to new Scarborough study. Available at: http://www.scarborough.com/press_releases/Cell%20Phone%20Ownership%20Increase%203.18.02.doc. Accessed August 16, 2004.
45. Chang BL, Bakken S, Brown SS, et al. Bridging the digital divide: reaching vulnerable populations. J Am Med Inform Assoc. 2004; 11:448–57.
46. Healy E. GSM fuels a cell-phone industry awaiting 3G. *Electronic Design*. Available at: http://www.elecdesign.com/Articles/ArticleID/2419/2419.html. Accessed August 16, 2004.
47. In-Stat MDR. 3G deployment better late than never. In-Stat and MicroDesign Resources (MDR). Available at: http://www.instat.com/press.asp?ID=919&sku=IN0401274GW. Accessed August 16, 2004.
48. GSA. The numbers add up with GSM and WCDMA. Global mobile Suppliers Association (GSA). Available at: http://www.gsacom.com/news/gsa_166.php4. Accessed October 26, 2004.
49. ISO. ISO 7816-2 (1988): Identification cards—integrated circuit(s) cards with contacts, Part 2: dimensions and locations of the contacts. Available at: http://www.cyberd.co.uk/support/technotes/smartcards.htm. Accessed October 26, 2004.
50. ISO. ISO/IEC 7816-3 (1989): Identification cards—integrated circuit(s) cards with contacts, Part 3: electronic signals and transmission protocols. Available at: http://www.cyberd.co.uk/support/technotes/smartcards.htm. Accessed October 26, 2004.
51. ISO. ISO/IEC 7816-1 (1988): Identification cards—integrated circuit(s) cards with contacts, Part 1: physical characteristics. Available at: http://www.cyberd.co.uk/support/technotes/smartcards.htm. Accessed October 26, 2004.
52. ETSI. Digital cellular telecommunications system (Phase 2+); specification of the subscriber identity module—mobile equipment (SIM-ME) interface. GSM 11.11 version 6.2.0 Release 1997. Available at: http://www.3gpp.org/ftp/Specs/archive/11_series/11.11/1111-620.zip. Accessed October 26, 2004.
53. Paying for fuel via mobile phone. Mobitel, Ljubljana, Slovenia. Available at: http://www.mobitel.si/eng/Press/PressReleases/Browsingbycategories/16Feb2004.asp. Accessed August 20, 2004.
54. Perttula K-P. UMTS security. Helsinki University of Technology. Available at: http://keskus.hut.fi/opetus/s38153/k2003/Lectures/g42UMTS_security.pdf. Accessed August 16, 2004.
55. Campbell R, Mckunas D. Analysis of third generation mobile security. Computer Science Department University of Illinois at Urbana-Champaign. June 28, 2002. Available at: http://choices.cs.uiuc.edu/MobilSec/posted_docs/3G_Security_Annual_Report.ppt. Accessed August 16, 2004.
56. Robinson A. Israeli scientists crack GSM mobile call security. Reuters. Available at: http://www.onlinesecurity.com/links/links568.php. Accessed August 16, 2004.
57. 3GPP. 31.102 V3.12.0 (2003-03) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM Application (Release 1999). Available at: http://www.3gpp.org/ftp/Specs/archive/31_series/31.102/31102-620.zip. Accessed August 16, 2004.
58. 3GPP. 3G TR 33.900 V1.2.0 (2000-01) Technical Specification 3rd Generation Partnership Project; Technical Specification Group SA WG3; A Guide to 3rd Generation Security (3G TR 33.900 version 1.2.0). Available at: ftp://ftp.3gpp.org/TSG_SA/WG3_Security/_Specs/33900-120.pdf. Accessed August 16, 2004.
59. NHII. Cornerstones for electronic healthcare. National Health Information Infrastructure 2004. Available at: http://www.hsrnet.net/nhii/materials.htm. Accessed August 16, 2004.
60. RSA. RSA SecurID tokens—the gold standard in two-factor user authentication. Available at: http://www.rsasecurity.com/node.asp?id=1157. Accessed August 16, 2004.
61. WAP Forum. Wireless application protocol WAP 2.0—technical white paper (January 2002). Available at: http://www.wapforum.org/what/WAPWhite_Paper1.pdf. Accessed August 16, 2004.
62. Foley L, Foley J. Identity theft: the aftermath 2003. A comprehensive study to understand the impact of identity theft on known victims. Identity Theft Ressource Center (ITRC). Available at: http://www.idtheftcenter.org/idaftermath.pdf. Accessed August 16, 2004.