AuthenLink: A User-Centred Authentication System for a Secure Mobile Commerce

Christina Braz[1], Esma Aïmeur[2]

[1] Department of Mathematics and Industrial Engineering, École Polytechnique de Montréal, C.P. 6079, succ. Centre-Ville, Montreal (Quebec) Canada H3C 3A7

[2] Department of Computer Science and Operations Research, University of Montreal, C.P. 6128, succ. Centre-Ville, Montreal (Quebec) Canada H3C 3J7

Abstract. We envision an environment where humans communicate directly with computers without additional authentication inputs like passwords, passphrases, PINs (Personal Identification Numbers), biometrics, or other existent authentication systems; and where humans *network* (intercommunicate) continually with wireless (mobile) devices. In this paper, we propose a new mobile authentication system, not yet implemented, called "AuthenLink", coupled with a new approach to distinguishing characteristics to authenticate people (authentication factor): something you CONVEY. The utmost purpose of this paper is to provide an ease, user-centred and acceptable security authentication system against fraud, counterfeit, and theft for the mobile commerce (m-Commerce) domain, more specifically for mobile devices. Our authentication system achieves its goal through a microprocessor chip (ChipTag) computer implanted under human skin. This ChipTag is able to authenticate user's access to systems, connect them wirelessly, through the Radio Frequency Identification (RFID) technology, and enable mobile devices perform mobile transactions, access files, or shop online.

1 Introduction

Mobile devices like mobile phones, Personal Digital Assistants (PDAs), hand-held devices, Portable Communications Services (PCS), and 3G devices[1] are now capable of retrieving email, managing our calendar, browsing the Web, using instant messaging, viewing media, playing games. Moreover, they afford us occasionally supply document processing, printing, and scanning abilities. In fact, the possibilities provided by mobile devices have been seen as a new paradigm: Mobile Computing. Mobile Computing implies the "availability" concept, which refers to the omnipresence of anytime, anywhere [1]. Furthermore, companies are, in an increasing degree, using a variety of mobile devices to store crucial business information, boost productivity, and improve customer relationships to achieve the competitive advantage. The

---

[1] 3G is a short term for third-generation wireless, and refers to a new wireless standard promising increased capacity and high-speed data applications up to two megabits, especially for mobile communications.

statistics on the mobile commerce (m-Commerce) industry are loud and clear. According to Forrester Research, the m-Commerce revenues for the global market is growing each year and will reach a US\$ 22 billion in 2005 against US\$7.5 billion achieved in 2003.

The authentication process is one of the basic frameworks of computing security. Thus, to enable a mobile device to distinguish between legitimate and non-legitimate users, most authentication systems provide passwords to authorize mobile users.

The primary issue is the lack of usability and acceptable security authentication system against fraud, counterfeit, and theft for mobile electronic transactions. The ability to securely trade business or shopping online and wirelessly is dependent on securely authenticating participants and digitally signing transactions.b

This paper presents a new mobile user authentication system called AuthenLink, designed for mobile devices, which integrates a microprocessor chip [2], a ChipTag, implanted under human skin and a mobile device antenna-embedded. AuthenLink gives the user automatic access to different resources in an acceptable secure authentication process, especially against fraud, counterfeit, and theft. In this way, a legitimate user will be able to conveniently prove her/his identity through the Radio Frequency Identification2 (RFID) technology, and gain access to the wireless network without threatening the safety of the organization. Furthermore, this article introduces a new approach to distinguishing characteristics to authenticate people, which we consider a fourth authentication factor: something you CONVEY.

This paper is structured as follows: We begin with a quick overview of the Pervasive and Mobile Computing issues in Section 1. Then, we define an authentication system, the usefulness role of a strong authentication and the authentication factors in Section 2. We describe the state-of-the-art of the authentication systems industry in section 3. Afterwards, we illustrate the technology overview of our system in section 4, while in section 5 we present the Architecture Usage Scenarios for the AuthenLink. Then, we describe the security aspects of our system in section 6. We validate our assumptions in Section 7 with an empirical evaluation of our system in comparison of other authentication systems. In Section 8, we state our reasoning for proposing a new mobile authentication system and a new authentication factor. Finally, the last Section presents the conclusions, and outlines opportunities for future work.

2 Authentication

Authentication is the process of establishing whether someone is who he or she declares himself or herself to be. In private and public computer networks (encompassing the Internet), authentication is popularly done through the use of logon passwords. The logon is the process used to get access to an operating system or application, generally in a remote computer. Usually a logon requires that the user have a user ID (username) and a password.

---

[2] Radio Frequency Identification (RFID) is a method of identifying unique items using radio waves. Typically, a reader communicates with a tag, which holds digital information in a microchip.

Authentication is one of the critical elements of a set of services that constitute a security sub-system in a communications infrastructure and encompasses the following security services: Authentication, Confidentiality, Integrity, Non-repudiation, Access Control, and finally Availability.

2.1 Strong Authentication Issues

Strong authentication refers to systems that require rigorous user identity verification, which is realized through multiple factors for authentication and employs advanced technology. The goal of strong authentication is to reinforce the security by replacing the classic authentication method of password for a software-only authentication solution with dynamic password generators, or software-hardware authentication solutions like smart cards, tokens, biometrics, etc. The greatest challenge of strong authentication is to make fraud more difficult for an attacker while respecting the constraints associated with an applications technical, economical, and organizational environment.

Until very recently, the suitable method for strong authentication was a smart card. For good reason, smart cards use Public Cryptography Infrastructure (PKI) digital certificates - the standard for digital authentication and signatures [3], which steadily protect the user's private key with hardware. However, certain characteristics of smart cards do not support the needs of today's business environment. These include the following: Lack of omnipresence (end-users are severely limited by the need to have access to card readers), Difficult to deploy (costly to administrate, and support), Expensive not cost-effective for large, distributed user communities.

Finally, an organization's authentication service should be suitable to the risks, and should consider the impact on users, as well as the cost of integration with its existing technology architecture, and total cost of ownership.

2.2 Authentication Factors

An authentication factor is Authentication Information (AI), information used to set up the validity of a claimed identity, utilized to check an identity demanded by or for a user. Consider the following scenario: before a Reliable Security System (RSS) gives Bob (a legitimate user) access to a computer system, network, or secure resource, the RSS must determine who he is, if he belongs to this system, if he has the right to access the system, and if he is the person he says he is. Actually, the RSS has demanded three distinct elements – *identification, authentication, and authorization* – that all together comprise the so-called *access control*. However, how does the RSS confirms that Bob is who he says he is? For example, entering his password does not prove it is him. Hence, the RSS needs the AI to authorize access for Bob. The AI may be gathered from one of the following authentication factors, as shown in Table 1. We can notice that associating two or more factors presents greater security (i.e. A PIN and a smart card). In this way, an authentication system using a single authentication factor may be vulnerable, but it depends on the employed technology. Our system will demonstrate that a single authentication factor is also possible.

Table 1. Authentication Factors.

Classification (NCSC-TG-017 [3])	Factor	Examples
Type 1: Authentication by Knowledge	Something only the user KNOWS	. Password or passphrase. . Personal Identification Number (PIN) . Information about the user or family members.
Type 2: Authentication by Ownership	Something only the user POSSESSES	. Physical key . Magnetic-stripe card . A token that generates a One-Time Password (OTP)
Type 3: Authentication by Characteristic	Something only the user IS (or does)	A Biometric trait: . Fingerprint . Iris pattern . Hand geometry . Voice
Or combination of the above		

3 Related Work

As of this writing, there is no related work developed that performs exactly as our system does, especially client's side. However it is important to present an overview relative to existing authentication methodologies on the market.

3.1. Passwords and PINs

For user authentication to an information system, the use of a password is by far the most common knowledge-based, Type 1 (See Table 1), authentication method. A long password, especially one with inserted spaces, is called a *passphrase*.

3.2. Authentication Tokens

Authentication Tokens (ATs) supply a means of authenticating and identifying an end-user. End-users protect their identity by using a physical object that is unique to them, for example, using a driver's license to prove a person's identity. To verify the identity of the token's owner, the host system performs its authentication protocol using data encoded on the token.

ATs come in a variety of physical forms. The size, shape, and materials from which a token is manufactured are referred to conjointly as the token's form factor. There are three main types of token form factors: Non-Contact Tokens (demand no electrical or physical contact with a token reader device such as proximity cards, One-Time Password generators, and handheld challenge-response calculators), Contact Tokens (make physical contact with the reader device like magnetic stripe tokens

---

[3] NCSC-TG-017 is a "Guide to Understanding Identification and Authentication in Trusted Systems", published by the U.S. National Computer Security Center (http://security.isu.edu/pdf/idenauth.pdf).

used in Automated Teller Machines (ATM) and Smart Card and Public Key Authentication.

3.3. Biometrics

Biometrics is a form of authentication that uses the user's physical or behavioural characteristics to verify his or her claimed identity. Physical characteristics like fingerprints, retinas and irises, palm prints, facial structure, and voice are some of the several existing biometric authentication methods.

3.4. Kerberos

An interesting variant of the authentication methods shown herein is Kerberos. It was created by MIT as a solution to network security problems [U1]. Kerberos is a network authentication protocol that supplies strong authentication and shares temporary base secrets for client/server applications by using secret-key cryptography. Authenticating mobile computing users might demand a considerable amount of processing and communications resources. Hence, research efforts have been directed towards developing some adaptations in this protocol in order to provide a better performance of public key-enabled Kerberos authentication in mobile computing applications [4].

Yet another sub-variant of the MIT-Kerberos authentication scheme is the security protocol [5] in which assigns authentication keys to the mobile nodes, dynamically thus, overcoming the problems related to static passwords in traditional schemes.

4   Technology Overview - AuthenLink

Those entire authentication methods described above have security problems: they lack usability, security (especially against fraud, counterfeit, and theft), and evolutivity. An authentication method must be flexible, interoperable, and anticipate the user's needs leaving an open door for future developments.

Our system is focused strongly on the user-side not on hardware itself. It is the result of the integration of a wireless semiconductor integrated circuit (IC) that stores an ID number in its memory (Chip_User_ID), implanted under human skin, and the mobile device antenna-embedded. This latter device will authenticate the user by making a connection between him or her, and the authentication server.

The main AuthenLink's components are the ChipTag, Radio Frequency Identification (RFID) technology, Mobile Reader, Authentication Server, and Database.

5 Architecture Usage Scenarios

In order to implement AuthenLink, we can make use of three distinct scenarios [U3]: UMTS[4] Architecture Mode (Maximum Mobility), WLAN[5] Architecture Mode (Medium Mobility), and Ad Hoc[6] Architecture Mode (Minimum Mobility). All of these scenarios can be implemented by an enterprise or an organization. In fact, the choice depends on the cost the enterprise or organization is willing to incur in terms of equipment, administration system, and human resources. In this paper, however, we focus on the UMTS Architecture Mode (Maximum Mobility) according to Figure 1. Let us see how it works:

Step 1: When the Mobile Reader (MR) antenna-embedded, is activated, say, when the ChipUser turns on the MR, it radiates a small amount of radio frequency energy through its antenna onto the ChipTag. Note: In this case, the Mobile Reader is a cellular phone.

Step 2: Radio frequency energy passes through the skin energizing the inactive ChipTag, which then emits a radio frequency signal conveying the ChipUser's unique ID to the MR for the purposes of user authentication. Using the energy it receives from the signal when it enters the radio field, the ChipTag will briefly converse with the MR for verification and data exchange. The ChipTag has no power supply, and a tiny transmitter on the ChipTag sends out the data (unique ID).
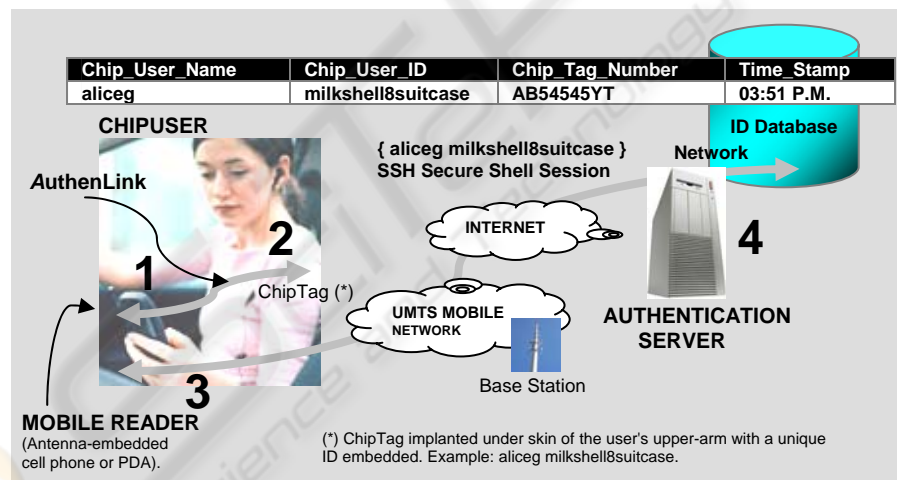

Fig. 1. UMTS Architecture Mode (Maximum Mobility).

Step 3: Once that data is received by the MR, it automatically authenticates the ChipUser's ID with the Authentication Server (AS) by means of a Base Station (Cell

---

[4] It is a third-generation (3G) broadband, packet-based transmission of text, digitized voice, video, and multimedia at data rates up to 2 megabits per second (Mbps) that offers a consistent set of services to mobile computer and phone users no matter where they are located in the world.

[5] WLAN is a local area network (LAN) without wires.

[6] ADHOC architecture is a networking framework in which devices or stations communicate directly with each other without the use of an Access Point (AP).

Phone Tower), and an UMTS Mobile Network, through the Internet. An SSH (Secure Shell) session automatically logs the ChipUser onto a remote AS [6]. The ChipUser gives his or her public key to the AS and then, when it connects, the AS knows access is permitted and automatically enables the connection. In fact, SSH uses a public/private encryption system to authenticate the ChipUser to the AS without the intervention of the ChipUser. We merely need to create a public/private key pair for the ChipUser, and then store the public key on the AS. Then, our SSH session client can use that key pair to automatically authenticate the ChipUser to the AS.

Step 4: Once the data is received by the AS, it can be sent to the database for processing and management. Linking each ID from the database to the ChipUser is performed.

6   Security

In this Section, we describe only the security issues[7] to be implemented between the Mobile Reader (RFID Technology) and the ChipUser.

In the RFI industry we have seen a huge effort to protect consumer privacy by securing information from "eavesdropping" or intercepting data exchanges. The main difference between RFID and, for example, a magnetic stripe technology (bank cards) is operability Over-the-Air (OTA8). The risk of eavesdropping, or intercepting, conveyed data is well acknowledged as is, for example, someone using a hide and malicious mobile reader. These risks are greatly reduced through the design of appropriate Over-the-Air protocols and data encryption methods. This protocol requires the Chip-Tag to be within range of both the mobile reader and the eavesdropper. Moreover, the mobile reader changes frequency quickly and the eavesdropping reader has to follow precisely the main mobile reader. In fact, this task is very difficult due to the randomness of the hopping sequence. Then, there is the data encryption algorithm code, which must be cracked to use the data. A well-designed system will protect consumers by implementing the proper protocol to achieve a level of security comparable and even beyond more evolved technologies.

7   Empirical Evaluation

There is no implementation of the AuthenLink system but we did carry out an empirical evaluation and comparison analysis of the authentication methods related to our system. In this way, we present in this section, an empirical evaluation of the authentication methods in comparison of our system (See: Table 2) with respect to different features encountered in other authentication methods.

---

[7] A complete description of the security mechanisms between the mobile reader and the authentication server can be seen at http://www27.brinkster.com/chbraz/index.html

[8] Over-the-air (OTA): is a standard for the transmission and reception of application-related information in a wireless communications system. OTA messages can be encrypted to ensure user privacy and data security.

Table 2. Comparative Analysis of the Authentication Methods

FEATURES	AUTHENTICATION FACTORS						
	Autthen Link	User-names & Passwords	OTPs/ Challenge Response	Tokens	Smart Cards & PKI	Biomet-rics	Kerberos
Accessibility	●	⊗	●	⊗	⊗	○	○
Durability	●	●	●	○	○	○	●
Mobility	●	●	●	●	●	○	⊗
Reliability	○	○	●	●	●	○	●
Performance	●	○	●	○	○	○	○
Security	○	○	●	●	●	○	●
Flexibility	●	●	●	●	●	○	○
Tamper-proof	●	⊗	⊗	●	●	○	●
Ergonomics	●	⊗	○	○	○	●	⊗
Privacy	○	●	○	●	●	○	○
Data Integrity	○	●	○	○	⊗	○	●
Ease of deployment	⊗	○	○	○	⊗	⊗	⊗
Interoperability	●	●	○	●	●	○	○
Compatibility	●	○	○	○	○	○	⊗
Extendability	●	○	○	○	○	○	⊗
Architecture Model	●	N.A.	○	⊗	⊗	○	●

In each authentication method, we rated the "features" on a Very-good (●), Fair (○), and Poor (⊗) basis. For a description of the advantages and disadvantages of the Au-thenLink go to: http://step.polymtl.ca/~chbraa/advantagesDisadvantages.htm

8 Discussion

A critical question arises from this analysis: Why do we need another user authentica-tion system, or further, a new authentication factor?

In today's mobile computing environment, solutions that provide an authentication system supported by combining several authentication factors are limited because they may be viewed as extremely cumbersome by the mobile user: something you KNOW, something you HAVE, and something you ARE. Passwords, passphrases, PINs, smart cards, and authentication tokens may be stolen, counterfeited, damaged, misused, and intercepted directly from the authentication system. Furthermore, we cannot trust biometric authentication on an unreliable wireless network unless we distribute base secrets (installed in the biometric reader) to authenticate the biometric readers [7]. Indeed, that's a cumbersome two-authentication factor. Moreover, each mobile user leaves a trace of his or her fingerprints, voice, and appearance wherever he or she goes.

A multi-factor authentication is another technical hurdle for a mobile user. In fact, it hides the weaknesses of distinct techniques (passwords, tokens, biometrics, etc.) by compounding two or more authentication factors in one mechanism [8].

As we can see, it is crucial to introduce a new mobile authentication system that improves security especially against fraud, counterfeit, and theft, and gives people on

the move fast and easy transactions. Therefore, we will introduce AuthenLink, a mobile one-factor authentication system; a new approach to authenticate people by distinguishing characteristics, which we consider a fourth authentication factor: Type 4 - Authentication by Emanation: something you CONVEY.

The user authentication main task in AuthenLink is made on the client side (ChipUser), and our effort is to internalize the authentication keystone process directly to an individual (chip is implanted under the skin of the user) instead of internalizing it to hardware (mobile device). Hence, we are confident that the base secret originates from a reliable source – the ChipUser.

Target group

AuthenLink could primarily be implemented to perform mobile access control with a variety of security, defence, financial, homeland security, and high-level secure-access applications such as government, research centres, business, and organizations. It could also be appropriated to m-Commerce to allow end-users to perform mobile electronic transactions. AuthenLink has to target the most tech-savvy mobile users such as Innovators, Technology Enthusiasts, and Early Adopters. They are the main target group for AuthenLink. However, our system is not suitable to Skeptics consumers.

Implications on the User Experience

The use of an authentication chip embedded beneath a person's skin may sound pedantic, or a little techy. In fact, it is. However, when the Social Security Number (SSN) was implemented in North America in 1935 as an all-purpose identifier (ID), people worried that the government would use it for other purposes. Some suspected that we could be tracked and linked to one another with sensitive data. Today, the vast majority of North Americans support some form of national identification like the Health Insurance Card, Driving Permit, or Social Security Card. If we accept a National ID system as we have accepted SSNs, five years from now the idea of an authentication chip may not appear as threatening as it does today. As with SSNs, people will get used to it.

Other people may be concerned about privacy because of the possibility that governments may, in future applications, implement an RFID tracking system to locate every citizen at any time. Let us consider the colossal infrastructure costs for a government institution to track all citizens, not to mention the massive database that would have to be generated. In fact, the viability of an application like this is beyond any government's capability. At present, in the U.S., one must obtain a court mandate to use private information like cell phone records and credit card purchases. Hence, the data generated from the use of RFID would be considered private and include the same privacy protections that are in place today [U2]. "The notion of embedding an authentication device in one's body is an interesting one. The U.S. government has recently passed regulations approving the implantation of such devices in humans" (Smith, R.E., personal communication, 2003[9]).

Finally, there is no way to control what could be realized, for example, with a biometric authentication or, with any other authentication system. "The problem is a

---

[9] R. E. Smith, Information Systems Security Consulting. Web Site: http://www.smat.us/crypto/index.html, Minnesota, USA, personal communication, July, 2003.

simple one: computing equipment is completely amoral and cannot tell whether it is being used for "good" or "bad" purposes. If a system can find an identity based on a biometric signature, then there is no purely technological way of controlling WHY a given search is performed. Given enough collusion among system operators and proprietors, there is always a way to fool the system into performing its function for unintended purposes" [9].

9 Conclusions and Future Work

The m-Commerce "channels" are being inundated with more electronic information than ever before. The open networks, which are easily accessible and inexpensive, surpass the more expensive and functionally limited communications channels. Since open networks are intrinsically less secure than private networks, secure m-Commerce depends largely upon information security itself (ChipTag implanted under skin) rather than channel security. Hence, the m-Commerce aims a mobile authentication method that is user-friendly, flexible and adequate security in order to boost the m-Commerce industry. AuthenLink is a single authentication factor, which provides an acceptable degree of security against fraud, counterfeit, and theft. Another major point is that AuthenLink is strongly focused on usability (easy user authentication) in order to take away much of the burdensome job of memorization and typing in usernames and passwords from users.

A fundamental sign that things are changing for new techy-savvy-based systems like AuthenLink is that worries about security issues are moving from the corporate realm - where security traditionally has been a major issue - to the individual user level. Indeed, the end-users are becoming increasingly *corporate-wise* due to the fact that they urge to reap the benefits of the technological advancements in a more secure way, and it is going to be tough for them to keep pace of those advancements due to the technological complexity. They aim an authentication system that is not complex to understand and use [10], and that is available on an ongoing basis. Definitely, this pronounced shift reinforces our belief that this is a significant factor in the growing trend of the acceptance of a user-centred system. The AuthenLink provides usability and always-on authentication system, speed and performance, flexibility, and contributes to the consolidation of the m-Commerce industry.

Following the investigations described in this work, a number of projects could be taken up. The concept of using AuthenLink for mobile authentication could also be extended to include a range of consumer products such as PCs, cars, and even homes and apartments. Furthermore, the authentication ChipTag could not only be used as an implant in a human being but also be attached to the mobile device, desktop, laptop, or any computer system as a hardware component. Another considerable improvement would be the possibility to allow the ChipTag be not "read only" (information can only be read, never changed) but read/write providing thus numerous promising applications.

Developing a secure and ease of use authentication system that can handle diverse, mobile device authentication represents our major challenge. In this work, we have taken the first step toward meeting this challenge by examining the need for a user-

friendly and secure mobile authentication system especially against fraud, counterfeit, and theft.

References

1. Pierre, S., Réseaux et systèmes informatiques mobiles – Fondements, architectures et applications, Presses Internationales Polytechnique, École Polytechnique de Montréal (Quebec) Canada (2003).
2. Bassiouni, M. & Mukherjee, A., A VLSI Chip for Efficient Transmission and Retrieval of Information, ACM Journal of the ACM, Department of Computer Science University of Central Florida Orlando, Florida 32816 - USA, (1987).
3. Burnett, S. & Paine, S., RSA Security's Official Guide To Cryptography, RSA Press, McGraw-Hill Companies, Berkeley, California - U.S.A. (2002).
4. Harbitter, A. & Menascé, A., The Performance of Public Key-Enabled Kerberos Authentication in Mobile Computing Applications, Proceedings of the 8th ACM (Journal of the ACM), Conference on Computer and Communications Security, Philadelphia, PA - U.S.A., Session: Mobile Code and Distributed Systems, pp. 78 – 85 (2001).
5. Raman, B. & Ramanathan, A., Artificial Intelligence Based Authentication Scheme for Mobile Adhoc Networks, White-Paper Dept. of. Computer Science/Dept. of Electrical Engg. - Texas A&M University, College Station, Texas 77843 U.S.A. (2001).
6. Barrett, D. & Silverman R., SSH, The Secure Shell - The Definitive Guide, 1st Edition, O'Reilly & Associates, Inc., 101 Morris West, Sebastopol, CA – U.S. (2001).
7. Smith. E. R., Authentication: From Passwords to Public Keys, Addison-Wesley, Addison-Wesley, 1st edition U.S.A. (October 1, 2001a).
8. Smith. E. R., Authentication: From Passwords to Public Keys, Addison-Wesley, Addison-Wesley, 1st edition U.S.A. (October 1, 2001b).
9. Smith. E. R., Authentication: From Passwords to Public Keys, Addison-Wesley, Addison-Wesley, 1st edition U.S.A. (October 1, 2001c).
10. Jøsang, A. & Patton, M. A., User Interface Requirements for Authentication of Communication, in the Proceedings of the Australasian User Interface Conference, Adelaide, Australia (February, 2003).

URLs:

U1 The MIT Kerberos Team, Kerberos: The Network Authentication Protocol (2004). http://web.mit.edu/kerberos/www/
U2 Hibbert, C., Frequently Asked Questions on SSNs and Privacy, Computer Professionals for Social Responsibility - Palo Alto, CA – U.S. (2004). http://www.cpsr.org/cpsr/privacy/ssn/ssn.faq.html
U3 Braz, C., AuthenLink's Architectures Usage Scenarios (2003). http://step.polymtl.ca/~chbraa/