Security Technologies in Mobile Networking

Jonny Karlsson, Arcada Polytechnic, Jan-Magnus Janssons plats 1, 00550 Helsingfors, Finland; E-mail: jonny.karlsson@arcada.fi
Göran Pulkkis, Arcada Polytechnic, Jan-Magnus Janssons plats 1, 00550 Helsingfors, Finland; E-mail: goran.pulkkis@arcada.fi
Kaj Grahn, Arcada Polytechnic, Jan-Magnus Janssons plats 1, 00550 Helsingfors, Finland; E-mail: kaj.grahn@arcada.fi
Robertino Hermansson, Arcada Polytechnic, Jan-Magnus Janssons plats 1, 00550 Helsingfors, Finland; E-mail: robertino.hermansson@arcada.fi

ABSTRACT

Specific security technologies for mobile applications and services – such as SIM/USIM/PKI SIM cards, hash chain generated security tokens for secure Mobile IP registration and mobile agent authorization, personal and public signature servers for mobile devices, and Identity based Public Key Cryptography (IdPKC) - are surveyed. Security solution examples and needed R&D are presented. A test environment for Mobile IP security solutions using IdPKC is also proposed.

1. INTRODUCTION

Mobile networking includes both network node mobility (notebook computers, handheld PDA computers, and mobile smart phones) and network software mobility (mobile agents). Mobility also puts specific technological requirements on basic security services like authentication, authorization, and digital signing.

2. SMARTCARDS

Specific security components in user devices in mobile cellular networks are smartcards such as SIM, USIM, and PKI SIM. A SIM is a smartcard securely storing an authentication key identifying a GSM network user. A PKI SIM is a SIM with an integrated RSA co-processor and storage space for private keys. A USIM is a SIM used in 3G mobile telephony networks, such as UMTS. Apart from authenticating users to cellular networks, these smartcards also are used in other security services.

2.1 SIM Card Based Authentication to Internet Services

Authentication to Internet services mostly occurs with the vulnerable username/password method. SIM based authentication is more secure and also convenient because of the widespread use of mobile phones with SIMs. In (Schuba et al., 2004) is proposed a SIM based approach with authentication protocols using an Identity Provider (IDP) Server operated by a mobile network operator. The SIM is accessed directly from the mobile phone, through a Bluetooth link to the phone, or through a WAP Proxy Gateway.

2.2 Secure Mobile IP Registration Protocol

In (Haverinen et al., 2001) GSM authentication based on the secret key in the SIM is proposed for a secure version of the Mobile IP Registration Protocol (Perkins, 2002). The AAA protocol (Glass et al., 2000) is used to access the GSM network through a proxy server, the GSM Authentication Gateway (GAGW), which translates between the Internet AAA protocol and GSM protocols. Two Mobile IP registration round trips are required. The RANDs of the subscriber are obtained and the GSM algorithm is executed on the SIM card. Finally, the actual authentication occurs. The system has been successfully tested with

- the GAGW implemented on Windows NT
- the GAGW connected to a GSM test network
- Windows 2000 and Linux based mobile nodes.

This Mobile IP Registration Protocol is also a standardization proposal in an IETF draft (Haverinen, 2001).

2.3 SSL Integration with SIM/USIM Cards

An Over-The-Air (OTA) connection to a SIM uses Application Protocol Data Unit (APDU) commands/responses (ISO/IEC 7816-4, 2005) encapsulated in protected SMS messages. APDU communication occurs in a SSL protected GPRS/TCP channel in the communication architecture described in (Badra and Urien, 2004). The Bearer Independent Protocol (BIP), defined in the European Telecommunication Standards Institute (ETSI) specifications TS 102 223 and TS 102 124 (ETSI, 2007), is required in the mobile device with the SIM. A modified SSL Handshake Protocol, in which certificate authentication is replaced by pre-shared secret based authentication, is proposed. BIP implements conversion from APDU commands/responses to SSL Handshake Protocol messages and to data sent over the SSL channel. An EAP-TLS based Authentication and Key Agreement Procedure (AKA) is proposed for a mixed WLAN-3G environment (Kambourakis et al., 2004). The SSL Handshake Protocol uses the AAA server certificate in the home network of the mobile device.

2.4 SIM Based Mobile PC Access

In (Mäkinen et al., 2001) architectures are proposed, where mobile phone SIMs and PKI SIMs are used for access to a mobile PC, which communicates with a remote server using the SSL protocol. A remote loader (RL) applet has been developed for SIMs implemented on Java cards. The RL applet supports communication to and from the SIM over an infrared link or over GSM.

2.5 Mobile Electronic Identity

Mobile FINEID, an electronic ID for inhabitants in Finland, is based on a Mobile Signature Service (MSS) and PKI SIMs allowing users to authenticate to online services and create digital signatures with private PKI SIM keys (Finnish, 2006). Currently, PKI SIMs are issued by two Finnish operators. PKI SIM owner identities are verified by mobile citizen certificates issued by the Finnish Population Register Centre (PRC) and attached to the private PKI SIM keys.

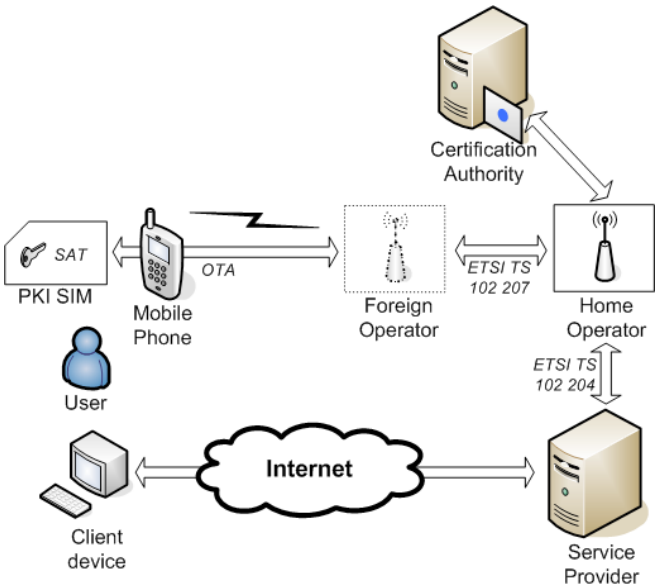
2.5.1 Technical Features of a FINEID PKI SIM Card

A FINEID PKI SIM contains a crypto processor and two PIN code protected private keys: an authentication/encryption key and a signature key. The corresponding certified public keys are stored in a directory administered by the PRC. Hashes of both public keys are stored in a PKI SIM for retrieval of correct certificates from this directory. The PKI SIMs are SIM Application Toolkit (SAT) enabled (3GPP, 2004) and contain a SAT application known as Wireless Internet Browser (WIB) (SmartTrust Case Studies, 2006). A PKI plug-in, PKCS#7 Signature Plug-In, executes cryptographic operations with the private keys through function calls executed by the WIB (SmartTrust White Papers, 2006). Function calls to and retrieval of return data from the PKCS#7 Signature Plug-In are encapsulated in SMS messages transmitted over an OTA connection.

2.5.2 MSS Architecture

The architecture of a Mobile Signature Service (MSS) is shown in Figure 1. Routing and roaming are based on public European standards. Thus, the Finnish mobile citizen certificate can in theory use any European MSS. Roaming and collaboration

Figure 1. MSS architecture



is ETSI TS 102.207 standardized, communication between the service provider and the mobile operator is based on an ETSI TS 102.207 standardized web service interface (ETSI, 2007). The interface is mainly based on SOAP (Simple Object Access Protocol), XML, and HTTP/HTTPS.

A workgroup of Finnish Federation for Communications and Teleinformatics (FiCom) has published a recommendation defining the rules for services using mobile citizen certificates and prescribing the technical interfaces for operators and service providers (FiCom, 2005). This recommendation is an application instruction for the ETSI standards TS 102 204 and TS 102 207. Extensions and adjustments to these standards are defined for limiting misuse. The purpose is to use electronic signature services independently of service providers and operators.

Example: User Authentication to a Protected WEB Service

1. The user tries to access the web service using HTTP and the web service informs the user that authentication is required and asks for the user's phone number
2. After receiving the phone number the service provider (in this case the web service) sends a signature request message, containing the user's phone number, to the mobile operator.
3. The mobile operator sends a signature request to the user's mobile phone PKI SIM, where a PKCS#1 signature is generated with the private key.
4. The PKCS#1 signature and the public key hash is sent back to the mobile operator and the user's citizen certificate is retrieved from the PRC directory based on the hash.
5. The signature is embedded into a PKCS#7 package, containing the user certificate, and sent to the service provider.
6. After successful signature verification, the user can access the protected WEB service

2.5.3 Evaluation

Currently, there are no public services for mobile FINEIDs. The architecture of current MSS systems is complex because of required SMS communication with the PKI SIM. An agreement between the service provider and the mobile operator is required for implementation services for mobile certificates. The technical specifications of operator specific PKI SIMs are confidential. Application and service development is thus mostly operator dependent.

Figure 2. Mobile signature and authentication service based on local PKI SIM access using OTA over Bluetooth

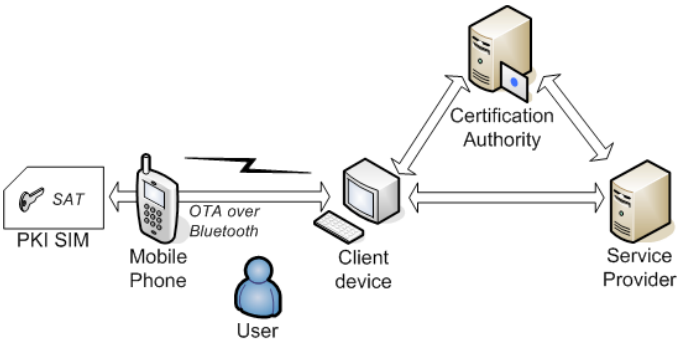
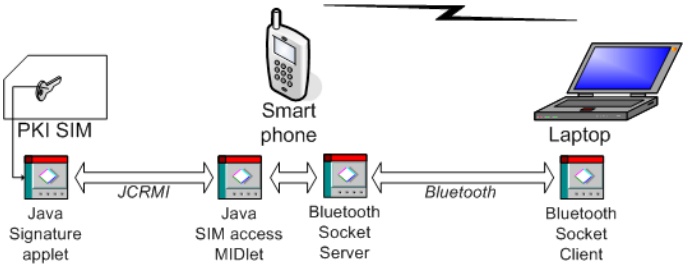


Figure 3. Bluetooth based Local PKI SIM access using the JCRMI protocol



2.6 Local PKI SIM Access

The purpose of research in Arcada Polytechnic is to develop a convenient and secure PKI SIM based signature and authentication service based on local PKI SIM access. A PKI SIM and mobile phone would then be equivalent to a smartcard in a smartcard reader. The user's client device would have PKI client functionality and the service would be operator independent. Two local PKI SIM access approaches are explored.

2.6.1 Approach for Current PKI SIM Cards

An approach is based on a proposal in (Mäkinen et al., 2001). An application residing on the user's client device (e.g. notebook computer) accesses the PKI SIM over an OTA connection using a short-link such as Bluetooth as data bearer, see Figure 2.

2.6.2 Prototype PKI SIM Supporting Access from a Java MIDlet.

A prototype PKI SIM supporting local access to PKI functionality from a smart phone application is proposed, see Figure 3.

An applet in a Java PKI SIM provides a method for signing with the private key. This method can be called remotely from a Java MIDlet installed in the smart phone using the Java Card Remote Method Invocation (JCRMI) protocol (JSR 177 Expert Group, 2004). This proposal supports the use of both the smart phone as well as a PC as a client device. When a PC is used as client device, authentication and signature data are transmitted between the smart phone and the PC over a Bluetooth channel.

3. HASH CHAIN GENERATED SECURITY TOKENS

Current network security standards propose X.509 certified PKI tokens for authentication and authorization services. However, security services based on such tokens are computationally heavy and require reliable real-time connectivity to updated Certificate Revocation Lists (CRLs). More lightweight security tokens are therefore needed by mobile network nodes and mobile agents, which usually

have limited computational and power capabilities. Lightweight tokens can be generated with one-way functions, for example as hash chains with Lamport's one-time password protocol (Lamport, 1981). Hash chain security depends on the used hash functions. Collision attack resistant hash functions are SHA-256, SHA-384, and SHA-512 with message digests of 256, 384, and 512 bits respectively (Stallings, 2006, p. 353).

3.1 Secure Mobile IP Registration

The Mobile IP registration protocol (Perkins, 2002) is in (Choi et al., 2004) protected from replay and man-in-the-middle attacks by Certificate Authority (CA) certified one-time public key authentication. The Mobile Node (MN) is authenticated by the Foreign Agent (FA) of the visited network and the FA by the Home Agent (HA) in the home network of MN. One-time public keys for MN and for each FA are generated with a one-way function from nonces chosen by HA combined with shared secrets between {MN, HA} and {each FA, CA}. The CA issues certificates for these public keys. From the CA, FA receives the public MN key certificate and HA the public FA key certificate. HA chooses and sends to the CA a new nonce during this message exchange. Both public keys and their corresponding certificates are updated by the CA after each iteration. A one-time public key (K_p) is in (Choi et al., 2004) calculated by

$$K_p = f^t(h(K_s, N_{HA})) \quad (1)$$

where K_p is the public key, K_s is a shared secret between {MN, HA} or {a FA, CA), N_{HA} is a nonce chosen by HA, h is a public hash function, and $f^t(x)$ means t successive applications of a public one-way function f to x, for example $f^5(x) = f(f(f(f(f(x)))))$.

The owner of a shared secret K_s (MN and each FA) publishes for authentication purposes a random i and $w_i = f^t(h(K_s, N_{HA}))$, where $0<i<t$. The owner is authenticated if

$$K_p = f^{t-i}(w_i) \quad (2)$$

where K_p is the corresponding public key (Choi et al., 2004).

3.2 Authorization Tokens for Mobile Agents

Authorization tokens implemented by hash chain values are proposed in a methodology called CADAT (Chained and Delegable Authorization Tokens) for mobile agent applications. Access rights are defined by issued *authorization certificates* and published hash chain values. An *authorization authority,* a controller of a set of n permissions, generates from a initial seed message m a hash chain of length n $\{h^0(m), h^1(m), h^2(m), \ldots, h^n(m)\}$, where h is a hash function, $h^0(m) = m$, and $h^i(m) = h(h^{i-1}(m))$ for $i = 1,2,\ldots,n$. Each hash value represents a permission. The authorization authority and users are assumed to have {public, private} key pairs and are represented by their public keys. An authorization authority issues a *chain contract certificate* to user A, who controls a mobile agent. User A issues for the needs of the mobile agent a *token contract certificate* to a remote host. User A then publishes the tokens to grant permissions for the mobile agent to be installed on the remote host and to access resources or services on the remote host. A hash of the mobile agent code can be included in the initial seed message of the hash chain and used to authenticate the mobile agent on the foreign host platform. The mobile agent requires no cryptographic operations to access remote host platform resources. A significant advantage of CADAT is, that mobile agents must not carry sensitive information such as cryptographic keys or even access tokens. (Navarro et al, 2004)

4. SIGNATURE SERVERS FOR MOBILE DEVICES

A signature server is often necessary for digital signing with a mobile device with limited computational and power capabilities. Two signature server solutions have been proposed, Personal Signature Server (PSS) and Public Signature Server. A PSS must require strong user authentication before a signature is created and the user of a Public Signature Server must be unambiguously identified in digital signature verification.

4.1 PSS

In (Campbell, 2003) is described a PSS installed on the personal workstation of a user. The private signing key is stored and used in a USB connected computer chip. The PSS is contacted using the HTTPS protocol. The PSS authenticates the user and sends a Java applet to the remote device. With the applet the user

- selects the document to be signed
- computes a hash of the document
- sends the hash to the PSS.

The PSS asks the user to validate the signature request with an encrypted message containing a unique token and a fingerprint of the document to be signed. After reception of a reply message with confirmed validation, the PSS creates the digital signature, stores a copy of it, and returns it to the remote device. Signatures are verified by a separate applet, which doesn't need the PSS if the public signing key is available. Revoking an existing signature key pair and generation of a new signing key pair is done at the console of the workstation with the PSS. The PSS keeps track of signed documents, stores and makes available older public keys for signature verification purposes. PSS vulnerabilities are evaluated in (Campbell, 2003).

4.2 Public Signature Server

A non-repudiation technique, called Server-Supported Signatures or S^3, based on one-way hash functions and traditional RSA digital signatures, is introduced in (Asokan et al., 1997). If h is a hash function, then a hash chain of length $n>0$ is expressed as n successive applications of h to x, $h^n(x)$, for example $h^5(x) = h(h(h(h(h(x)))))$. A hash function is "personalized" by including a user identity in x. Then h(x) actually means h(ID_user,x). If $x = K_s$ is chosen to be a private user key, then $h^n(K_s)$ is the public key. If a hash value $h^i(K_s)$, $0<i<n$, is published when a signature is created, then the signer can be identified by checking that a hash chain of the published value gives the public key. Thus n represents the maximum number of signatures, which can be created with a hash chain.

A CA is needed to define unambiguously which Signature Server (S) creates a S^3 signature. S and CA create own private/public key pairs. A user of an S must send his/her user_ID, public key K_p, maximum number of signatures n, and the address of S to the CA, which creates a public signed certificate for the delivered information. A server-aided PKI infrastructure service (SaPKI) to create S^3 signatures for mobile clients in GSM and UMTS networks has been used in a "cell phone banking" application. (Cai et al., 2005).

The Public Signature Server in (Lei et al., 2004), using RSA key pairs with an exponent e=3, creates/verifies signatures more efficiently than the S^3 technique in (Asokan et al., 1997).

The security of creating/verifying signatures is thus based on

- uncompromised private keys
- the use of secure hash functions like SHA-256
- sufficient RSA key lengths.

5. MOBILE SECURITY SOLUTIONS BASED ON IDPKC

In Identity based Public Key Cryptography (IdPKC) any string representing a user or device identity can be used as a public key from which a private key can be derived with a secret master key. Thus public key use requires no certification by a trusted third party and no CRLs are needed. Security services based on IdPKC rather than on X.509 certified PKI are therefore suitable for mobile devices with limited computational and power capabilities – especially since efficient IdPKC based encryption/decryption algorithms exist (Hwu et al., 2006).

5.1 IdPKC Basics

IdPKC was first introduced in (Shamir, 1984). The basic IdPKC operation is *pairing* e(P,Q), which is defined for a pair of discrete points, P,Q, on an elliptic curve. Elliptic Curve Cryptography (ECC) is described in detail for example in (Menenez, 1994). This pairing operation is proved to be *bilinear* with respect to discrete point addition:

$$e(P1+P2,Q) = e(P1,Q)*e(P2,Q), e(P,Q1+Q2) = e(P,Q1)*e(P,Q2) \quad (3)$$

Thus $e(2*P,Q) = e(P,Q)^2 = e(P,2*Q)$ and $e(a*P,b*Q) = e(b*P,a*Q) = e(P,Q)^{a*b}$. Two types of pairing operations, Weil Pairing and Tate Pairing, exist (Maas, 2004).

The first IdPKC scheme with satisfactory security is proposed in (Boneh and Franklin, 2002), Encryption/decryption operations are Weil Pairing based. The security level of these operations is the same as for ECC based encryption/decryption operations.

$Q_{ID} = s*H_1(ID)$ is the public key of a user or a network node and the corresponding private key is $d_{ID} = s*Q_{ID}$, where

- ID is a public identity string, for example a mobile phone number or a Network Access Identifier (NAI) with the format username@domainname or devicename@domainname
- H_1 is a hash function converting an ID to a discrete point Q_{ID} on a chosen elliptic curve.
- s is a secret master key, randomly chosen by a trusted third party called *Private Key Generator (PKG)*, which securely distributes d_{ID} to a user or to a network node.

IdPKC based encryption/decryption and signing/signature verification algorithms are described in detail for example in (Lee et. al., 2003). IdPKC security is evaluated in (Maas, 2004).

5.2 IdPKC Based Mobile Security Solutions

In (Lee et. al., 2003) is proposed a secure version of the Mobile IP registration protocol in (Perkins, 2002). An AAA server authenticates the MN and the MN authenticates the HA by signature verification. In (Hwu et al., 2006) Weil Pairing algorithms presented in (Boneh and Franklin, 2001) are tuned for some elliptic curves over the binary fields $GF(2^{163})$, $GF(2^{233})$, and $GF(2^{409})$. The evaluated performance improvement is about 30%. An IdPKC scheme based on the tuned algorithms is proposed for protected end-to-end data communication between mobile smart phone users.

A test environment for mobile security solutions using IdPKC and standard AAA protocols has been built in Arcada Polytechnic, see Figure 4. Solutions proposed in (Lee et al., 2003; Hwu et al. 2006) will be implemented, tested and evaluated for existing open source and commercial Mobile IP software. The security protocols in these solutions will also be formally verified.

6. CONCLUSIONS

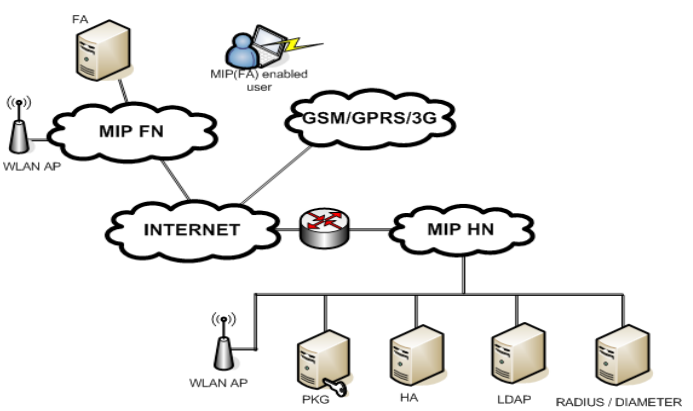
The SIM/USIM/PKI SIM cards in mobile devices in GSM/UMTS networks constitute a key technology for authentication services and digital signing in mobile networking. Other current security technology trends for mobile networking are

- the use of hash chains and IdPKC as lightweight alternatives to X.509 certification based PKI technology
- the use of signature servers for digital signing with mobile devices.

An essential mobile security service is secure Mobile IP registration for which still not standardized solutions based on SIM cards, on hash chains and on IdPKC are proposed.

More research on security requirements of mobile networking is needed, since current standardization of security solutions for mobile networking is quite insufficient for the needs of present and future mobile applications and services.

Figure 4. Test environment for Mobile IPv4 Software supporting IdPKC and an AAA protocol



REFERENCES

3GPP (2004). Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment. Retrieved January 5th, 2007, from http://www.3gpp.org

Asokan, N, Tsudik, G and Waidner, M. (1997). Server-supported signatures. *Journal of Computer Security.* Vol. 5, Issue 1, pp. 91-108.

Badra, M. and Urien P. (2004). *Toward SSL Integration in SIM SmartCards.* Wireless Communications and Networking Conference WCNC. Vol. 2, pp. 889 – 893

Boneh, D. and Franklin, M. (2001). *Identity-Based Encryption form the Weil Pairing.* Lecture Notes of Computer Science vol. 2139, Springer-Verlag, pp. 213-229.

Cai, L., Yang, X., and Chen, C. (2005). *Design and Implementation of a Server-aided PKI Service (SaPKI).* Proc. 19th International Conference on Advanced Information Networking and Applications, AINA 2005. Vol. 1, pp 859-864

Campbell, S. (2003). *Supporting Digital Signatures in Mobile Environments.* Proc. Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises WET ICE. pp. 238 - 242

Choi, D.H., Kim, H., and Jung, K (2004). *A secure mobile IP authentication based on identification protocol.* Proc. 2004 International Symposium on Intelligent Signal Processing and Communication Systems ISPACS. pp. 709–712.

ETSI Publications Download Area (2007). Retrieved January 8th, 2007, from http://pda.etsi.org/pda/queryform.asp

FiCom. (2005). FiCom RY:n soveltamisohje ETSI:n MSS-standardeille V1.1. Retrieved June 8th, 2006, from http://www.ficom.fi

Glass, S., Hiller, T., Jacobs, S., & Perkins, C. (2000). *Mobile IP Authentication, Authorization, and Accounting Requirements*. IETF, RFC 2977.

Haverinen, H. (2001). *GSM SIM Authentication and Key Generation for Mobile IP*. IETF draft. Retrieved June 9th, 2006, from http://www.iptel.org/ietf/security/draft-haverinen-mobileip-gsmsim-02.txt

Haverinen, H., Asokan, N., and Määttänen, T. (2001). *Authentication and Key Generation for Mobile IP Using Gsm Authentication and Roaming.* Proc. IEEE International Conference on Communications ICC. Vol. 8, pp. 2453-2457.

Hwu, J.-S., Chen, R.-J. & Lin, Y.-B. (2006). *An Efficient Identity-based Cryptosystem for End-to-end Mobile Security*. IEEE Transactions on Wireless Communication, Vol. 5, No. 9, pp. 2586-2593

ISO/IEC 7816-4:2005 Part 4. Retrieved June 9th, 2006, from http://www.iso.org

Kambourakis, G., Rouskas, A., Kormentzas, G., and Gritzalis, S. (2004). Advanced SSL/TLS-baseds authentication for secure WLAN-3G internetworking. *IEE Proc.-Commun.,* Vol. 151, No 3, pp. 501-506

Lamport, L. (1981). *Password Authentication with Insecure Communication.* Comm. ACM, Vol. 24, No. 11, pp. 770-772.

Lee, B.-G., Doo-Ho Choi, D.-H., Kim, H.-G., Sohn, S.-W. Park, K.-H. (2003). *Mobile IP and WLAN with AAA authentication protocol using identity-based cryptography*, 10th International Conference on Telecommunications ICT, Vol. 1, pp. 597 - 603

Lei, Y., Chen, D., and Jiang, Z. (2004). *Generating Digital Signatures on Mobile Devices.* Proc. 18th International Conference on Advanced Information Networking and Applications AINA. Vol. 2, pp. 532-535.

Maas, M. (2004). *Pairing-Based Cryptography*. MSc Thesis, Technische Universitet Eindhoven, The Netherlands.

Menenez, A.J. (1994). *Elliptic Curve Public Key Cryptosystems.* USA: Kluwer Academic Publisers. ISBN: 0-792-39368-6

Mäkinen, S., Bessler, F., Wiedmer, E., Kehr, R., Schmidt, R., Bonnet, J., Lobo, C., Vieira, F., Brady, M. (2001). Towards Secured Service Access. Retrieved June 9th, 2006, from http//www.eurescom.de

Navarro, G, Garcia, J., and Ortega-Ruiz, J.A. (2004). *Chained and Delegable Authorization Tokens.* Proc. Ninth Nordic Workshop on Secure IT System – Encouraging Co-operation, NORDSEC2004, Espoo, Finland, pp. 8-14.

JSR 177 Expert Group. (2004). Security and Trust Services API (SATSA) for Java™ 2 Platform, Micro Edition, Specification: JSR-177 Version 1.0 (Final Release). Retrieved June 10th, 2006, from http://www.jcp.org/en/jsr/detail?id=177

Perkins, C. (2002). *IP Mobility Support for IPv4*, IETF, RFC 3344.

Schuba, M., Gerstenberger, V., and Lahaije, P. (2004). *Internet ID – Flexible Re-use of Mobile Phone Authentication Security for Service Access.* Proc. Ninth Nordic Workshop on Secure IT System – Encouraging Co-operation, NORDSEC2004, Espoo, Finland, pp. 58-64.

Shamir, A. (1984). *Identity-based cryptosystems and signature schemes*. Lecture Notes in Computer Science vol. 196, Springer-Verlag, pp. 47-53

SmartTrust Case Studies. (2006). Case study: Elisa. Retrieved January 8th, 2007, from http://www.smarttrust.com/mobile_solutions/mobile_solutions_case_elisa.asp

SmartTrust White Papers. (2006). SmartTtrust WIB™ Plug-ins Specification. Retrieved January 8th, 2007, from http://www.smarttrust.com/mobile_solutions/mobile_solutions_wp_wib.asp

Stallings, W. (2006). *Cryptography and Network Security.* Fourth Edition. USA: Pearson Prentice Hall. ISBN 0-13-187316-4