A Survey on Mobile Digital Signature Models

Mohammad Hasan Samadani
Amirkabir Univ. of Technology
Computer and IT Dept.
mhssamadani@aut.ac.ir

Mehdi Shajari
Amirkabir Univ. of Technology
Computer and IT Dept.
mshajari@aut.ac.ir

Mehdi Ahaniha
Amirkabir Univ. of Technology
Computer and IT Dept.
mm.ahaniha@aut.ac.ir

ABSTRACT
The application of a fast and secure mobile signature model is an essential issue for the development of the mobile electronic commerce, since digital signatures can provide authentication, non-repudiation, and data integrity. There are several technologies and models with the aim of implementing signature processes for mobile devices. In this paper, we categorize them into client based and server based models. We will comment on the most important properties of each solution and analyze the advantages and disadvantages, with a special focus on the private key security, performance of the signature generation process, and application of digital certificates.

Categories and Subject Descriptors
A.1 [**Introductory and Survey**]; K.4.4 [**Computers and Society**]: Electronic Commerce – *security*; H.3.5 [**Online Information Services**]: Web-based services;

General Terms
Security

Keywords
Mobile Signature, Security, SIM Card, Mobile Device, Digital Certificate.

1. INTRODUCTION
Most of the m-commerce applications or services need to use some security services to guarantee the safety of the transactions that they perform. The most important security services are authentication, non-repudiation, and data integrity because of providing essential evidences proving participation of the correct user in a correct transaction. Authentication, non-repudiation and data integrity can be achieved using digital signatures and digital certificates.

ICEC'10, August 2-4, 2010, Honolulu, Hawaii, USA.

Mobile applications based on their security requirement may need one or more digital signatures in a specific period of time. For example, a mobile banking protocol proposed by D. Li, D. Lin, G. Zhao, and B. Huang [1] needs one digital signature in each of its transactions, but a secure mobile auction application may need to send several bids in a short period of time. So, it needs to generate several signatures in that period. Hence, the delay and time length of signing is very important in many types of mobile applications.

The private key protection and computational costs are the main challenges of efficiently deploying of digital signatures in m-commerce.

In the first generation of mobile clients, it was hard to generate digital signatures due to the limited cryptographic and computational capabilities of these clients. However, currently the mobile clients are able to generate digital signatures based on asymmetric cryptography [2]. A mobile client consists of a mobile device and a SIM card. In short, a SIM card is a smart card with an application which implements the GSM11.11 specification.

Both mobile devices and SIM cards are able to generate signatures and store keys. However, mobile devices has more powerful CPUs and can generate signatures faster than SIMs, but SIM cards are more secure to store the keys [2]. Also, mobile devices are more flexible than SIM cards.

There are many models and approaches to generate digital signature in m-commerce, and we can classify them according to several criteria such as signature platform, technologies, standards and supported features [2]. Also, we can classify mobile signatures based on where to generate the signature. Based on this, there are two possible mobile signing approaches: client based and server based mobile signatures.

In this paper, we discuss client based and server based mobile signatures. We compare these models with a special focus on the performance and the private key security.

The rest of this paper is organized as follows. Section 2 and 3 generally discuss server and client based mobile signatures, and summarize the related works. Section 4 presents the comparison of different signature models, and discusses the requirement of a secure and fast mobile signature model. Finally, section 5 concludes the paper.

2. SERVER BASED MOBILE SIGNATURES

Server based digital signature is a signature created by a signature service provider for a mobile client. This type of signatures is categorized into certificate based and certificate-less signatures.

2.1 Certificate Based Server Side Mobile Signature

Three types of certificates can be used in certificate based server side mobile signatures; the client's certificate, server's certificate, and proxy certificate.

2.1.1 Server Based Signatures with Client's Certificates

By using client's certificate, the client's private key will be revealed to the server and, therefore, this type of signature cannot be considered as a legal signature of the client [3]. Figure 1 illustrates such a server based signature. This model is like the SET Wallet Server model [4].

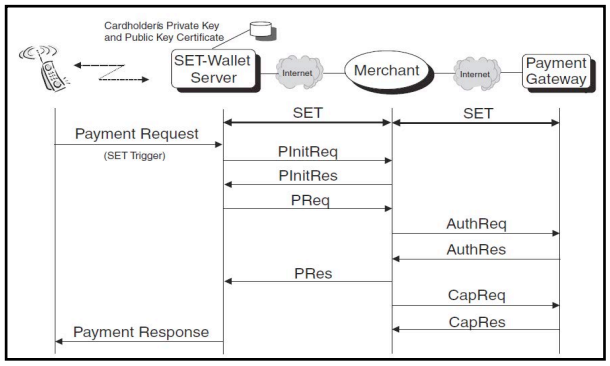

Figure 1. SET-Wallet Server model [4]

2.1.2 Server Based Signatures with Server's Certificates

The second type of server based signatures is produced using the certificates issued to the service provider. In fact, the signature service provider acts as a replacement for the client. Based on the signature of the provider, it cannot be verified that the client really authorized the signature and so this type of signature cannot be considered as a legal signature of the client [3]. Figure 2 illustrates this type of server based signature generation.

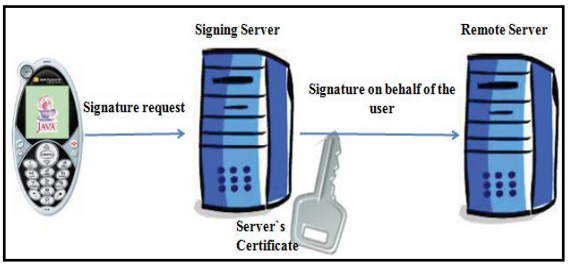

Figure 2. Server based model with server's certificate

In 2007, C.L. Chen, C.C. Chen, L.C. Liu, and G. Horng [5] proposed a server based mobile signature scheme that uses server's certificate. After that, in 2008, Z. Wang, Z. Guo, and Y. Wang [6] proposed a server based mobile signature that can be categorized as this type of server based signatures.

2.1.3 Server Based Signatures with Proxy Certificates

This type of server based mobile signatures is based on delegating the signing power to mobile agents using proxy certificates [7]. In this case, the user generates a key pair and the corresponding proxy certificate for the mobile agent and sends it to the service provider. In the remote server, the mobile agent has a private key and a proxy certificate so it can sign on behalf of the client. This signature can be assumed as the client's proxy signature.

In this scheme, the user's private key is not revealed to the server. However, an attacker can attack the agent and, therefore, the agent's private key may be revealed or misused. Also, the agent will be forced to generate illegal signatures. To solve this vulnerability, the validity period of proxy certificate is kept short and its signing capabilities and the number of times that the certificate can be used to sign are limited. These mechanisms can reduce the vulnerability of proxy signature and costs of misusing. However, they cannot solve the problem completely [8].

In 2001, A. Romao and M. Silva [9] used proxy certificates to delegate signature power to a mobile agent. After that, in 2004, O. Bamasak, N. Zhang [10] proposed a secure method for signature delegation to mobile agents. Their work is different from other related proxy signature schemes in that in addition to providing confidentiality protection to the proxy key, the method provides non-repudiation services to all the parties involved. Also, in 2007, C.M. Ou, and C.R. Ou [8] used proxy certificates to delegate signature power to a mobile agent in a mobile payment system.

2.2 Certificate-Less Server Side Mobile Signatures

A certificate-less server based mobile signatures consist of those signatures that are not based on regular signing algorithms like RSA and DSA. These innovative algorithms are based on dividing the signature generation computations in such a way that a signature is generated only with the cooperation of both client and server and the client's computational load is very low.

In 2003, K. Bicakci, and N. Baykal [11] proposed the SAOTS signature model for pervasive computing. After that, in 2005, they proposed Improved Server Assisted Signature [12]. In 2004, L. He, N. Zhang [13] proposed a novel server based signature protocol called Joint Signature. After that, in 2007, they improved their work by proposing Improved Joint Signature [14]. The IJS protocol enables a mobile user to delegate her signing power to an assisted server in a way that the assisted server can perform signature generation and verification on behalf of the user. The signature generated by IJS could be assumed as a joint signature of client and server which is generated by the server as according to user request. Also, in 2004, Y. Lei, D. Chen, and Z. Jiang [15] proposed the SBS model to generate the signature in a remote server for mobile devices. The SBS protocol is based on a hash chain that is generated by the mobile client, and does not use the general public/private key and standard digital certificates. Also, in 2007, X. Ding, D. Mazzocchi, and G. Tsudik [16] proposed the SAS signature model. The SAS is a signature method that relies

on partially trusted servers to generate signatures for regular mobile users.

Beside the key establishing problem, the most important drawback of these protocols is that they must be supported by the sender, receipt and server. Moreover, these protocols do not support the digital certificates and so cannot be used widely.

2.2.1 Improved Joint Signature (IJS)

The IJS protocol enables a mobile user to delegate her signing power to an assisted server in a way that the assisted server can perform signature generation and verification on behalf of the user. In the IJS, a session key, freshly established between the two end entities, and timestamps have been used. The high efficiency of the IJS at the mobile side has been achieved through the use of only two hash operations: the generations of HMAC and HOAC. The protocol shifts the processing load from the mobile side to the server and to the recipient, each of which performs two public key operations, one signature generation operation and one signature verification operation [8].

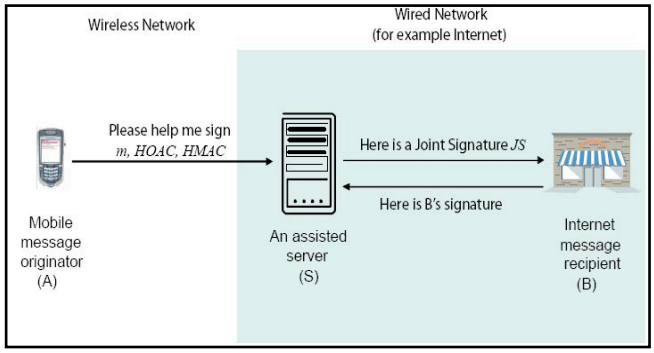

Figure 3. IJS protocol

The signature generated by IJS could be assumed as a joint signature of client and server which is generated by the server as according to user request. Beside the key establishing problem, the most important drawback of this protocol is that it must be supported by the sender, receipt and server. Moreover, this protocol does not support the digital certificates and so cannot be used widely. Figure 3 illustrates the IJS protocol.

2.2.2 Server-Based Signature (SBS)

The SBS protocol is based on a hash chain that is generated by the mobile client and does not use the general public/private key and standard digital certificates [23]. Figure 4 illustrates the SBS protocol. Like the IJS protocol, the SBS protocol must be supported by involved parties and cannot be widely used.

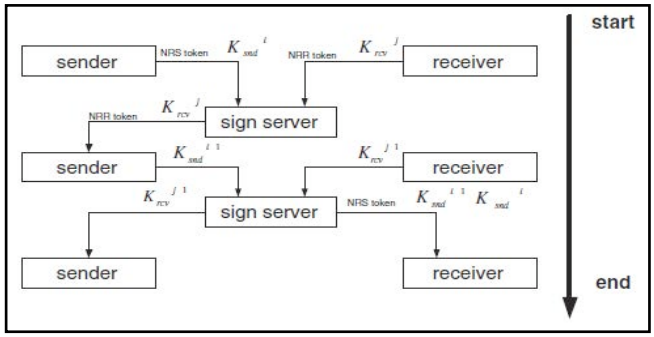

Figure 4. SBS protocol

3. CLIENT BASED MOBILE **SIGNATURES**

In the first generation of mobile devices, it was hard to generate digital signatures due to the limited cryptographic and computational capabilities of these devices. However, currently the mobile clients are able to generate digital signatures based on asymmetric cryptography [2].

A mobile client consists of a mobile device and a SIM card. Both the mobile device and the SIM card can generate signatures and store the keys. However, usually, a mobile device has a more powerful CPU and can generate signatures faster than SIMs, but a SIM card is more secure to store the keys. As both the mobile device and the SIM card can store the keys and generate the signatures, we can assume three models for client based signing based on key storing and signature generation location(s).

3.1 SIM Based Signature

In the SIM based model both of key storing and signature generation operation are done within the SIM card. Figure 5 illustrates this model.

As the SIM card has a very secure environment, this model guarantees the security of keys. The private key will never exit from the SIM. Therefore, it will not be revealed to anyone [2, 3]. However, the SIM cards are slow in generating digital signatures [2]. The invocation time of the SIM cards by the mobile device is also significant [17]. So, this model is very secure, but it is slow.

The SATSA-PKI [18] based signature, WIM application based signature [2], and Handset-based SET Wallet [4] are important examples of this type of signatures.

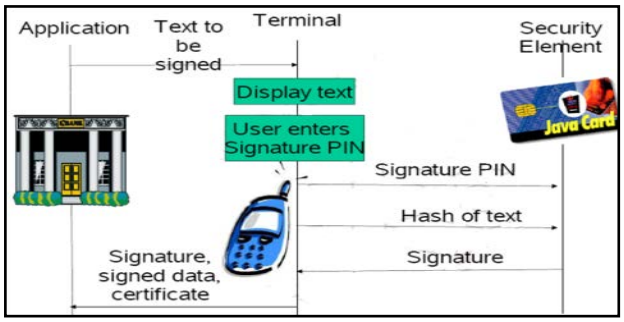

Figure 5. SIM based model

3.2 Device Based Signature

Another way to handle mobile digital signatures is the device based signature model. In this model, both the key storing and signature generation operations happen in the device. Storing the keys in the file system or some other storage locations in the device is not very secure because of security weaknesses of mobile devices and their operation systems. However, as the CPU of mobile devices is more powerful than SIM cards, the signature generation will be faster. Therefore, this model is very fast, but it is also very vulnerable at the same time. Figure 6 illustrates this model.

There are several libraries and tools that enable a mobile device to generate digital signature. The most important libraries are Bouncy Castle [19], IAIK Micro Edition [20], and SATSA-CRYPTO package [18].

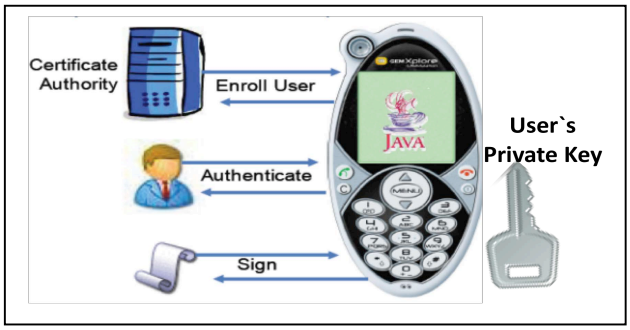

Figure 6. Device based model

3.3 Hybrid Signature

There are a large number of services that cannot be implemented completely in the SIM card side or in the device side. These services usually need to take advantage of the device characteristics (rich user interface and high processing capabilities) as well as the security of the SIM card [2].

In the hybrid model the keys are stored in the SIM card, but the processing of digital signature generation takes place in the device. As the keys are necessary for signing, in the time of signature generation, the keys must exit from the SIM card and be revealed to the device. This method is almost as fast as the device based signature. However, with regards to key security, it is less secure than the SIM based method and more secure than the device based signature. Figure 7 illustrates hybrid signature model.

This type of mobile signature is proper when the SIM card is only capable to store the keys, and it cannot generate digital signatures.

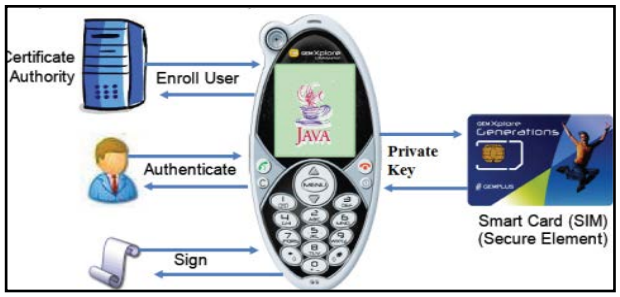

Figure 7. Hybrid model

4. COMPARISON OF MOBILE SIGNATURE METHODS

In the previous sections of this paper, we have discussed about two types of mobile signatures, the server based and client based models. As mentioned before, the server based mobile signatures are not promising signatures because of their shortcomings and drawbacks [3].

A.R. Martinez, D.S. Martinez, M.M. Montesions, and A.F.G. Skarmeta [2, 21] and Heiko Rossnagel [3] had mentioned that the future mobile signatures must be client based. As mentioned before, there are three types of client based mobile signatures in three different levels of security and performance. The SIM based one is the most secure as well as the most time consuming one. The device based model is very fast, but is not very secure because of vulnerability of the private key. The other one, the hybrid model, is almost as fast as device based model but with higher security. However, it is less secure than the SIM based model because the private key must be revealed to the device and, therefore, an attacker can take advantage of the revealed key.

In most of m-commerce applications and services, the user must generate only one or two digital signatures. Therefore, the SIM based signature model could be the best choice for signature generation. This model guarantees the security of user's private key, and the elapsed time is tolerable for the user. However, if the number of needed signatures increases, the elapsed time will seriously affects the user's performance.

There are some kinds of m-commerce applications that need several digital signatures in a short period of time, e.g. mobile auctions. These types of applications need fast, low delay and secure signatures. For example, in a secure auction, the client must send several non-repudiable bids in a short period of time, so the bids must be sent with very low delay, especially when the auction nears to be closed. As we mentioned before, the current mobile signature models are suffering from security or performance. Therefore, none of previously discussed mobile signature models is secure and fast enough to be used for these types of mobile applications. We have presented a new client based mobile signature model, the SPMS model [22], to overcome this problem.

5. CONCLUSION

The application of a fast and secure mobile signature model is an essential issue for the development of the mobile electronic commerce, since digital signatures can provide authentication, non-repudiation, and data integrity. There are several technologies and models with the aim of implementing signature processes for mobile devices. We have discussed about two types of mobile signatures, the server based and client based models. The server based mobile signatures are not promising signatures because of their shortcomings and drawbacks. And, the future mobile signatures must be client based.

There are some types of applications need fast, low delay and secure signatures. The current mobile signature models are suffering from security or performance. Therefore, none of currently used mobile signature models is secure and fast enough to be used for these types of mobile applications. Therefore, the developing a fast and secure client based mobile digital signature is essential for the m-commerce growth.

6. ACKNOWLEDGMENT

This work was supported by Iran Telecommunication Research Center. Our thanks to Antonio Ruiz-Mart´nez for his valuable comments and notes.

7. REFERENCES

[1] D. Li, D. Lin, G. Zhao, and B. Huang, "Design and correctness proof of a security protocol for mobile banking", Bell Labs Technical Journal, vol. 14(1), 2009, pp. 259-266, Alcatel-Lucent, Wiley Periodicals, doi: 10.1002/bltj.20366.

[2] A. Ruiz-Martinez, D. Sanchez-Martinez, M. Martinez-Montesinos, A.F. Gomez-Skameta, "A survey of electronic signature solutions in mobile devices", Theoretical and applied electronic commerce research, vol. 2, issue 3,December 2007, pp. 94-109.

[3] H. Rossnagel, "Mobile qualified electronic signatures and certification on demand", in: Proc. of the 1st European PKI Workshop, Samos, Greece, June 2004.

[4] O'Mahony, Donal; Peirce, Michael; Tewary, Hitesh, "Electronic payment systems for e-commerce", Artech House, 2001, chapter 8, pp. 302-325.

[5] C.L. Chen, C.C. Chen, L.C. Liu, G. Horng, "A server-aided signature scheme for mobile commerce", IWCMC07, ACM, Aug. 2007, USA.

[6] Z. Wang, Z. Guo, Y. Wang, "Security research on J2ME-based mobile payment", ISECS Int. Colloquium on Computing, Communication, Control, and Management (CCCM08), IEEE, 2008, pp. 644-648, doi: 10.1109/CCCM.2008.216.

[7] J. Claessens, B. Preneel, J. Vandewalle, "(How) Can mobile agents do secure electronic transactions on untrusted hosts?", ACM Trans. On Internet Technology, vol. 3, No. 1, Feb. 2003, pp. 28-48.

[8] C.M. Ou, C.R. Ou, "Adaptation of proxy certificates to non-repudiation protocol of agent-based mobile payment systems", Applied Intelligence, v.30 n.3, p.233-243, June 2009 , doi: 10.1007/s10489-007-0089-4.

[9] A. Romao, M. Mira da Silva, "Secure mobile agent digital signatures with proxy certificates", E-commerce Agents, LNAI 2033, Springer, 2001, pp. 206-220.

[10] O. Bamasak, N. Zahng, "A secure method for signature delegation to mobile agents", ACM Symposium on Applied Computing (SAC04), ACM, Mar. 2004, pp. 813-818.

[11] K. Bicakci and N. Baykal. "SAOTS: A New Efficient Server Assisted Signature Scheme for Pervasive Computing", LNCS No. 2802, Germany, 2003.

[12] K. Bicakci and N. Baykal. "Improved Server Assisted Signatures", Journal of Computer Networks, Elsevier, 2005, vol. 47, No. 3 pp. 351-366.

[13] L. He, and N. Zhang, "A New Signature Scheme: Joint Signature", Proceedings of the 2004 ACM symposium on Applied computing, Cyprus, 2004, pp. 807-828.

[14] L. He, N. Zhang, L. He, I. Rogers, "Secure m-commerce transactions: a third party based signature protocol", third int. Symposium on Information Assurance and Security, IEEE, 2007, doi: 10.1109/IAS.2007.66.

[15] Y. Lei, D. Chen, Z. Jiang, "Generating digital signatures on mobile devices", Proc. 18th International Conference on Advanced Information Networking and Application (AINA04), IEEE, 2004.

[16] X. Ding, D. Mazzocchi, G. Tsudik, "Equipping smart devices with public key signatures", ACM trans. On Internet Technology, vol. 7, No. 1, Article 3, Feb. 2007, doi: 10.1145/1189740.1189743.

[17] S.T. Chanson, T.W. Cheung, "Design and implementation of a PKI-based end-to-end secure infrastructure for mobile e-commerce", World Wide Web, vol. 4, 2001, pp. 235-253, Kluwer Academic Publishers.

[18] SATSA Development Guide, available at: http://java.sun.com/j2me/docs/satsa-dg.

[19] BouncyCastle Library, http://www.bouncycastle.org

[20] IAIK Library, http://jce.iaik.tugraz.at

[21] A. Ruiz-Martínez, Daniel Sánchez-Martínez, María Martínez-Montensiones, A. F. Gómez-Skarmeta. "Mobile Signature Solutions for Guaranteeing Non-Repudiation in Mobile Business and Mobile Commerce". Mobile and Ubiquitous Commerce: Advanced E-Business Methods: Volume 4 of Advances in Electronic Business Series. IGI Global Publishers. May 2009.

[22] M. H. Samadani, M. Shajari, M. M. Ahaniha, "self-proxy mobile signature, a new client-based mobile signature model", WAMIS'10, in Proceeding of the 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Perth, Australia, 2010.