Location Stamps for Digital Signatures: A New Service for Mobile Telephone Networks

Matthias Kabatnik[1] and Alf Zugenmaier[2]

[1] Institute of Communication Networks and Computer Engineering,
University of Stuttgart, Germany,
kabatnik@ind.uni-stuttgart.de

[2] Institute for Computer Science and Social Studies – Dept. of Telematics,
Albert-Ludwigs-University Freiburg, Germany,
zugenmai@iig.uni-freiburg.de

Abstract. Location aware services are expected to make up a large share of the mobile telephone market in the future. The services proposed so far make use of uncertified location information—information push services, guidance systems, positioning for emergency calls, etc. We propose a service that provides certified location information. Integrated with cryptographic digital signatures this service enables the determination of the current position of the signer in a provable way. Such certified location information—called location stamp—can be applied in electronic commerce, e.g. for determination of applicable laws or taxes.

1 Introduction

The benefit of modern cellular telephone networks is the ability of users to roam with their terminals being reachable at all times. The underlying system needs information about the user's location to be able to route calls to the mobile terminal. This information is provided by maintaining special registers that store information about the area and the cell where the user is located.

In cellular mobile communications networks like the GSM network the traffic volume is increasing steadily. However, the number of simultaneous calls per cell is limited. Therefore operators shrink cell sizes—at the hot spots like airports and train stations even down to picocells (several tens of meters in radius)—in order to keep up with the growing number of call attempts. Thus, location information of the mobile stations in the network becomes more accurate and enables services like location depended charging (low tariff in the so-called *home zone*). Other regulatory requirements (for example by the FCC) demand even more precise location information, e.g. to provide better emergency call response services. Therefore, mobile terminal tracking methods like triangulation with higher precision have been developed.

With the availability of precise location information new services are possible. One application of location information in daily business is signing of contracts. The location of signing may determine to which jurisdiction the contract is subject to. When manually signing a contract, it contains the location, the date, and the hand-written signature. The written location can be verified immediately since both contract partners are present; in an electronic commerce setting this location of the conclusion of a contract, i.e. where it is signed is not evident. How can one be sure where the partner is located?

We designed a new service that provides an approved location stamp bound to a digital signature in order to map the process of manual contract signing to modern communication systems. Additionally, we present a procedure that assures the correct mapping of the communications system's view on a mobile terminal to a user requesting a location stamp. In order to provide liability we make use of digital signatures based on asymmetric cryptographic algorithms.

The remainder of this paper is organized as follows: First we describe the service and the technical entities required to generate a location stamp that can be tied to a digital signature. In chapter three we show the protocol that can be used to perform this. In the next chapter we map this generic description to the functional and organizational entities of the GSM networks to show the feasibility of the service. Chapter five discusses security aspects of the protocol and shows its limits. The related work is presented in chapter six, and finally a summary is given.

2 Service Specification

The location stamp service (LSS) provides a location stamp which certifies at which position the subscriber is located when making a signature—or rather, at which position the subscriber's mobile station is visible to the network. This location stamp can be verified by any third party using the public key assigned to the LSS, and it can be used as a proof of the location information. In this scenario the service operator who signs the location is a trusted third party (i.e. the signer is neither the principal of the stamp nor the verifier of the stamp).

2.1 Location Measurement

There are two main types of location measurement: positioning and tracking. Positioning is a measurement which is performed within the mobile device (e.g. by an integrated GPS receiver). The calculation of the position is also done in the mobile device. The other type is tracking: Some external measurement infrastructure determines the position of the mobile device (e.g. by triangulation using the mobile's emitted signal).

Positioning has the advantage of greater accuracy, privacy of location information, and - for security critical applications like proving a location via a telecommunication channel - the disadvantage of requiring tamper proof hardware, and resistance against misleading the device with a fake environment like a GPS simulator. Tracking has the disadvantage of lower accuracy, possible loss of privacy against the network, but the advantages of being harder to deceive.

In our approach we have chosen tracking because it offers better security and because of its straightforward implementation: tracking information is available in a cellular telephone network since the location information is needed for routing and billing purposes.

2.2 Cryptographic Capabilities

The handwritten signature can be replaced by the digital signature in electronic commerce (e.g. [1]). A digital signature using asymmetric (public key) cryptography is created by calculating a hash of the document to be signed and encrypting this hash with the private key of the signer [2]. The signature can be verified by anybody who knows the public key of the signer. The private key has to be kept secret by the signer. To bind a public key to an identity, a certificate according to a standard like X.509 [3] is used. This certificate is signed by a certification authority that guarantees the fact that a certain public key belongs to the identity named in the certificate.

Next to the need of identification of users signing a contract there is the necessity to identify terminals within a network. This identification is needed to perform routing, addressing, and billing tasks. In mobile networks usually authentication mechanisms are provided to prove the terminal's claimed identity. Therefore, a mapping between the identity and some secret exists—usually a symmetric key—that must be known by the network.

We will use a generic identifier called MoID (Mobile IDentifier) and a secret key named K.

2.3 Binding Signature and Authentication

From the perspective of the network, only a terminal named by a non-ambiguous MoID can be located in the network. Because the task in our scenario is to certify that a certain person signs a document at a certain location, it is necessary to bind the capability to authenticate the user's identity to the same physical entity that is used to authenticate the identity of the mobile terminal. This can be done, e.g. by placing the private signature key and the key K corresponding to MoID on the same tamper resistant chip card. The chip card should also provide the capabilities for authentication and signing to prevent the keys from ever leaving the physical module. When both operations (proof of user ID with a signature and authentication of MoID) are performed at the same time, they must be performed at the same place. Thus, the location of the terminal is identical with the place of signature.

The physical binding of the two keys can be represented by a digital certificate issued together with the chip card.

3 Protocol

The location stamp protocol consists of six information flows which may consist of several messages each (e.g. in case of fragmentation or necessary acknowledgments). First the abbreviations are introduced, then the protocol itself is presented. The abbreviations used are:

MS	mobile system
LSS	location stamp service
LMS	location measurement system
H	hash value

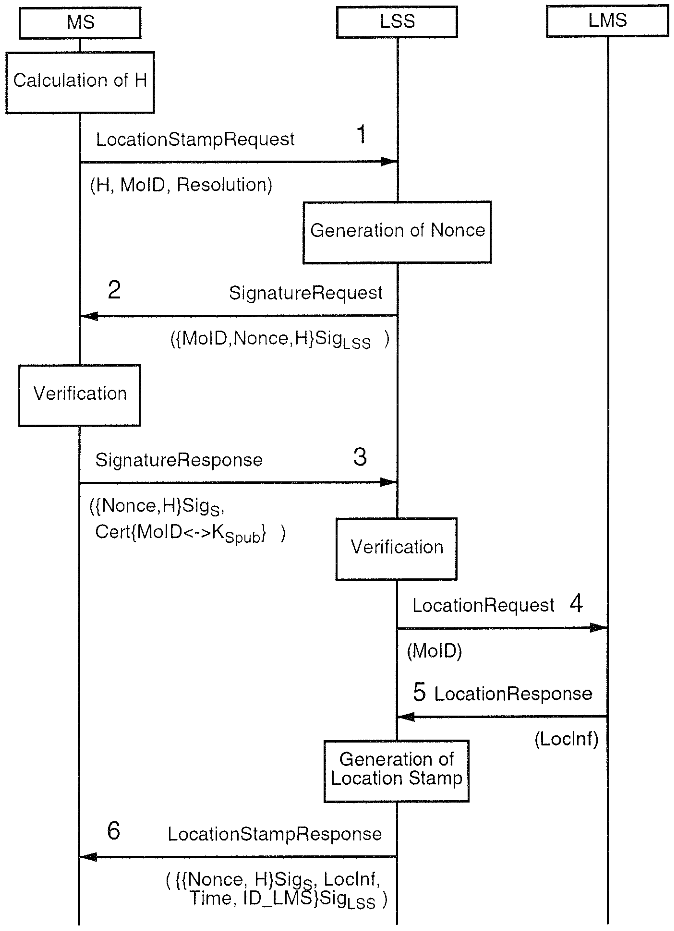

Fig. 1. Successful run of LSS protocol

MoID	mobile's identity
K_{Spub}	public key corresponding to the private key of the subscriber
{...}SigS	signature of the data in parenthesis with the private key of the subscriber
{...}SigLSS	signature of the data in parenthesis with the private key of the location stamp service
ID_LMS	identifier of the applied location measurement system (LMS)

An example of a successful protocol run is presented in Fig. 1.

The following explanations will refer to an information flow (IF) depicted by an arrow, and its preceding operation block (if any).

IF 1: The hash of the document is calculated. This can happen at any place at any time before the run of the protocol since the hash is simply another representation of the document that shall be signed. Thus, this calculation does not necessarily have to be performed within the mobile device. The mobile device initiates the protocol run by sending a service request to the service. The request contains the mobile's ID and the hash. The hash is included to provide some additional information for preparing the operation of IF 3. The communication between mobile and service can be settled on any kind of bearer service that is available. Additionally, the mobile supplies the desired resolution for the location stamp.

IF 2: The service generates a nonce value. A nonce is a kind of random value which may contain some time dependent information (e.g. 8 time related octets and 2 random octets). This value is used to prove recentness within the protocol [4]. If the mobile can generate a signature containing this nonce value, the service can derive that the counterpart has been alive after the reception of message 2. The message in IF 1 alone does not give this information since it could be a replay or a complete fake. The signature provided by the service is necessary to ensure that the nonce was produced by the service. Additionally the hash value within the message can provide the same effect like the nonce if it is unique (in cases when one document has to be signed several times an additional nonce value is necessary to protect against replay attacks). The signed nonce is sent to the mobile.

IF 3: First the mobile checks if the parameters H and MoID are the same as in IF 1. If this is not the case, no time consuming cryptographical operation has to be performed, the message can be discarded immediately, and the protocol terminates with an error. If the parameters fit, the signature of the service is validated. Now the mobile knows that the nonce was generated by the service and shall be used for signing the document represented by H. The mobile signs the concatenation of the document's hash H and the nonce, and sends the signature back to the service. Additionally, it may provide a certificate which can be used to prove the physical binding of the secret key belonging to its signature key $K_{S_{pub}}$ and the MoID. In order to reduce the amount of information that is transferred, this certificate may also be stored at the LSS.

IF 4: The LSS verifies the signature of the mobile to be sure of the origin of the value. Since the signature contains the nonce, it can be derived that it is fresh. The key used to produce this signature is located inseparably from the authentication mechanism of the MoID, therefore the service must locate the corresponding mobile station. The LSS prompts the location measurement system for the location of the mobile...

IF 5: ... and receives the location information.

IF 6: The LSS generates the location stamp by expressing the received location information with the accuracy requested by the mobile system in step 1 (resolution parameter). Additionally, the point of time is provided. The parameter ID_LMS is included to enable any verifier of the signature to apply his own estimation of the trustworthiness (cf. section 5.1). Finally, the mobile receives the requested location stamp.

4 Mapping onto the GSM Infrastructure

The GSM system, standardized by the ETSI in 13 series of standards [5], is used primarily in Europe and Asia. It has a share of about 65% of the world's digital cellular

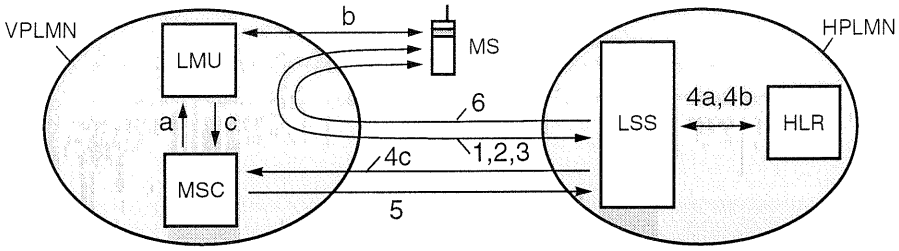

Fig. 2. Request for a location stamp by the mobile station. The figures and letters correspond to the information flows

telephone networks. Two types of mobility are supported by the GSM system: mobility within a network and mobility across networks (roaming). The location information that handles the mobility inside a network is stored in the visitor location register VLR of the network the mobile station is currently booked into. The home location register HLR in the network of the provider is used to store information about which network the subscriber is currently using. It also stores personalization parameters of services of the subscriber.

GSM enables subscriber mobility in a sense that different subscribers may use the same terminal. To bind a device to an identity, a subscriber identity module (SIM) is used. It is generally placed in a chip card or module that can be plugged into different terminals. On the SIM card the international mobile subscriber identification (IMSI), a 15 digit number, is stored. To address this subscriber, a mobile station ISDN number (MSISDN) is used. More than one MSISDN may be assigned to a subscriber identified by the IMSI.

Location information in the GSM network arises naturally: it is necessary to route a call to its destination. This information has a resolution of the cell size. In the GSM standard [6],[7] a location service (LCS) is described that permits a more precise measurement. A location service client may request the location of a subscriber that is identified by its IMSI or MSISDN. The location service can communicate with the location measurement units through the mobile switching centre (MSC) to locate the terminal device and return the current position to the LCS client.

4.1 Location Stamp in GSM Networks

We propose the following mapping of the technical entities of the protocol as described above to the entities that are available within the GSM system:

The IMSI takes the role of the MoID. The public key of the subscriber ($K_{S_{pub}}$) can be stored on the SIM card. This enables the network operator of the subscriber to issue a certificate that states the physical binding between the IMSI and $K_{S_{pub}}$. The HLR has knowledge which network the mobile station is booked into. The MSC of this network can contact the location measurement units which can in turn locate the mobile. The location measurement itself depends on the desired resolution: it is either possible to just locate the cell the mobile is booked into—this can be performed with a lookup—or

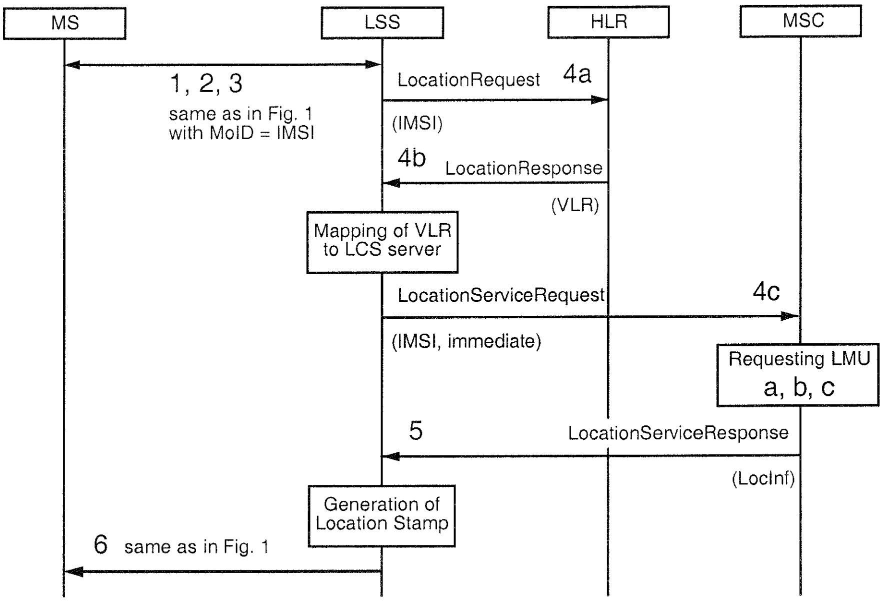

Fig. 3. LSS service in a GSM environment

perform a measurement, e.g. based on time of arrival of a signal emitted from the mobile station at two or three base stations. The measurement itself is performed by location measurement units, the result is calculated by the location service (LCS) server.

As a transport protocol for the connection between the terminal and the LSS Unstructured Supplementary Service Data (USSD) or even Short Message Service (SMS) can be used. In Fig. 2 the entities and the information flows between them are depicted. In Fig. 3 a trace of a successful protocol run in the GSM network is shown. The information flows are:

IF 1, 2, 3: Same as in chapter 3. The communication between mobile and service can be settled on any kind of bearer service that is available (e.g. GPRS, USSD). The certificate binds the public key K_{Spub} to the IMSI, thus stating that the private key K_{Spub}^{-1} is stored on the SIM card corresponding to the IMSI. In the case of GSM the retrieval of location information (IF 4 of Fig. 1) maps to several IFs denoted by an appended letter (a, b, c).

IF 4a: The LSS verifies the signature of the mobile to be sure of the origin of the value. Since the signature contains the nonce, it can be derived that it is fresh. Since the key used to produce this signature is located inseparably in the SIM with the IMSI assigned, the service must locate the corresponding mobile station. The LSS prompts the HLR for the location of the mobile station ...

IF 4b: ... and the HLR provides the routing address of the MSC currently serving the mobile, which is indicated in the data base entry indexed by the IMSI.

IF 4c: The LSS assesses this MSC address. The VPLMN may not support location services, or the LSS provider may not consider it to be trustworthy either for its poor protection of secrecy and integrity (possible manipulation of location data) or simply for the provided accuracy of the location information. In the latter case the LSS aborts the request by sending an error message to the mobile. However, if the MSC supports location services and is considered to be trustworthy the location information request is sent to the MSC in the immediate mode (only minimum delay between request and response is acceptable) which in turn uses the infrastructure of the VPLMN to perform the necessary measurements. We assume that all necessary steps like encryption or physical separation of network links are taken to protect the integrity of the communication between LSS and the infrastructure of the VPLMN.

IF a, b, c: The MSC determines the location involving one or more location measurement units (LMU)

IF 5: The MSC sends its answer to the LSS.

IF 6: The LSS generates the location stamp by expressing the received location information with the accuracy requested by the mobile system in step 1 (resolution parameter). Additionally, the point of time is provided. The parameter ID_LMS is included to enable any verifier of the signature to apply his own estimation of the trustworthiness of the LSS and the VPLMN. Finally, the mobile receives the requested location stamp.

In case the protocol cannot terminate successfully, an error is returned. There are two general types of errors: protocol internal errors and protocol external errors.

Protocol internal errors are related to the information flows 1-6. It is possible, that a message is not received in time or that some verification fails. In this case typical error messages can be generated and delivered to the participants of the protocol run.

Protocol external errors are related to the process of location measurement (IF a, b, c in the GSM example). These errors might be caused by either a negative judgement of the LMS with respect to the security qualities of the responsible LMS or simply by unavailability of location information with the desired accuracy. In cases low resolution information is available the LSS can negotiate with the requester and thus, recover from the error condition. In all other cases the protocol terminates without a stamp being delivered.

5 Security Considerations

Some reasoning about the security of the protocol has been given in chapter 3. In this section we discuss two additional security aspects of the service. Firstly, the trust model which can be expressed by assumptions made by the involved parties. Secondly, the possibility of subverting the service by tunnelling information.

5.1 Trust Model

When a location stamp is presented to an acceptor A, she may or may not accept the location stamp according to her trust in the parties involved in the provision of the stamp. The parties involved depend on the selection of the LSS by the requester of the stamp and the LMS in charge. In case of GSM the LMS depends on the network a mobile device is booked into. While the number of possible LSS with respect to a certain subscriber is rather limited (e.g. the LSS of the HLMNP of the GSM subscriber) the number of possible LMS can be large. Therefore, it is appropriate to look at trust in the LSS and the LMS separately.

Informally A trusts B concerning some action if A expects B to behave accordingly (with an acceptable probability). Yahalom et al. give a classification scheme of trust in [8]. They provide an open list of classes of trust like *providing good quality keys (kg)* or *Provide identification of one entity to another (id)*. We extend this list by the class of *Providing correct location information (cl)*[1].

If there was no indication of the source of the location information contained in the stamp, the acceptor of a location stamp would be forced to trust the LSS to provide good location information.

Since the LSS includes the ID_LMS in the stamp it states implicitly a recommendation regarding the cl-property of the LMS. By making the source of the location information visible, the acceptor A is enabled to restrict the set of possible location information sources. Thus, A can define a set SLSS of LSS, from which she is willing to accept stamps and recommendations, and—for each LSS—a set SLMS of LMS that she is willing to rely on.

An example of these restrictions could be the following: an acceptor A might think of a GSM network operator, who offers LSS1, that he has good insight in the technical quality of the location services (LCS) of the GSM networks that have roaming agreements with him. Thus, A accepts any recommendation of LSS1, i.e. any stamp issued by LSS1 with any source of location information will be accepted by A. In case of another operator, who may be new in the market, A restricts his trust in the recommendations of LSS2 to the LCS of the operator's own network.

There are other aspects of trust, we do not discuss in detail, since they are not visible to the acceptor A and therefore, she has to trust the LSS with respect to these points completely. To give some examples: A has to trust the LSS with respect to correctly authenticating the signature key corresponding to $K_{S_{pub}}$. The LSS has to trust the issuer of the certificate used to establish the relation between MoID and $K_{S_{pub}}$. In case of GSM the LMS has to trust the HLR and authentication centre (AuC) to provide correct challenges for the authentication of the mobile. All entities have to trust the used signalling network infrastructure to provide secure communication channels.

5.2 Relay Problem

When locating a certain mobile device, it is of importance, that the tamper resistant chip card is at the point of visibility, i.e. in the located device. If an attacker uses a manipulated mobile phone, which is able to tunnel the chip card's interface via another communications media to another place, this assumption is false and the system is subverted. In cases when this attacker scenario is relevant, additional mechanisms have to be provided. One possibility can be fraud detection systems, which can detect impossible changes of a subscribers location (e.g., a mobile booked into a network in Scotland

[1] The term correctness comprises accuracy and correlation between location information and given identity of the located subject, thus implicitly containing the id-property.

and signing some data in southern France at almost the same time). Another possibility is using more sophisticated physical measurements (e.g. response time limitation), which are beyond the focus of this paper. If this relay attack were staged, a physical presence of at least an air interface at the location to be spoofed is necessary. Evidence of this may be traceable at a later point of time.

6 Related Work

Other location aware services in the public land mobile network, like integration in intelligent transport systems [9], or road maps and directories [10] use the current location that is not certified by a third party. In certificates that are used for commercial transactions [3], the place of residence can be certified, but not the location where the current transaction takes place.

Tang, Ruutu, and Loughney briefly discuss the problem of lack of trust between different parties exchanging location information. They state the necessity of a trusted third party involved in the protocol [11].

A security relevant application of the location information is described in [12], where GPS is used for positioning an authentication device. The location information is then used as additional authentication information to decide whether access should be granted.

In the Internet increasing demand for locating the visitors of a web site has led to other location services. For example, the company quova.com [13] offers location information based on IP addresses for marketing purposes. Again this location information is not certified and the location information does not really state the position of the web surfer, it can only locate the last proxy the connection goes through.

Enhancing the digitally signed documents with a location stamp is similar to adding a time stamp to it. Different standards exist, one of them is the PKIX draft [14].

7 Summary

We have presented a new type of service enhancing the capabilities of mobile communication terminals. Extending digital signatures with location stamps provided by a trusted third party can be used to improve electronic commerce applications. Additionally, the new service enables other applications like electronic travel logs or proof of service for field staff. We have proposed a service architecture which can be realized with existing telecommunication networks. Therefore, only limited effort has to be taken to bring the service into existence.

References

1. Directive 1999/93/EC of the European Parliament and of the Council: A Community Framework for Electronic Signatures, December 1999
2. D. W. Davies and W. L. Price: The Application of Digital Signatures Based on Public Key Cryptosystems, Proceedings of the Fifth International Computer Communications Conference, October 1980, pp. 525–530

3. ITU-T Recommendation X.509 Data Networks and Open System Communications – Directory – Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, Geneva, June, 1997
4. Lowe, G.: A Hierarchy of Authentication Specification. In Proceedings of the 10th Computer Security Foundation Workshop. IEEE press, 1997
5. GSM 01.01: Digital cellular telecommunications system (Phase 2+); GSM Release 1999 Specifications, ETSI TS 101 855
6. GSM 02.71 Digital cellular communication system (phase 2+); location services; service description, stage 1, ETSI TS 101 723
7. GSM 03.71 Digital cellular communication system (phase 2+); location services; functional description, stage 2, ETS 101 724
8. Yahalom, R.; Klein, B.; Beth, Th.: Trust relationships in secure systems – a distributed authentication perspective. In Proceedings of the IEEE Conference on Research in Security and Privacy, pages 150–164, 1993
9. Shibuya, A.; Nakatsugawa, M.; Kubota, S.; Ogawa, T.: A high-accuracy pedestrian positioning information system using pico cell techniques; In: IEEE 51st Vehicular technology conference proceedings, Volume 1, pages 496–500, spring 2000
10. Hu, Yun-Chao: IMT-2000 mobility; In: Proceedings of the IEEE Intelligent Network workshop 2000, pp. 412–435, 2000
11. Tang, H.; Ruutu, J.; Loughney, J.: Problems and Requirements of Some IP Applications Based on Spatial Location Information, IETF draft ¡draft-tang-islf-req-00.txt¿, 2000
12. Denning, D.: Location-Based Authentication: Grounding Cyberspace for Better Security, Computer Fraud & Security, Elsevier Science, February 1996.
13. www.quova.com
14. Adams, C.; Cain, P.; Pinkas, D.; Zuccherato, R.:IETF draft <draft-ietf-pkix-time-stamp-12.txt>, December 2000