CERTILOC: Implementation of a spatial-temporal certification service compatible with several localization technologies

J.M. de Fuentes, A.I. González-Tablas, A. Ribagorda
Computer Science Department. University Carlos III de Madrid (SPAIN)
jfuentes@inf.uc3m.es, aigonzal@inf.uc3m.es, arturo@inf.uc3m.es

Abstract

Recently researchers are being encouraged to address security and privacy requirements for location information. This work contributes to this area by presenting the design and implementation of CERTILOC, a prototype of a spatial-temporal certification service that is interoperable with representative localization technologies (GSM Cell-ID and GPS). Our work is completed with a broad threat analysis on spatial-temporal certification services and an exposition of legal considerations that can be made if used in work scenarios.
Keywords. Certification, localization, legal issues.

1. Introduction

Nowadays a wide range of location estimation technologies are accessible to the general public. The most well-known location estimation technology is the Global Positioning System (GPS), probably followed by the cell-based location information provided by some wireless networks such as mobile phone networks. Supported on the spreading of location estimation technologies, location-based services are gradually becoming a reality. Some well-established examples include the enhanced emergency call services (such as 911 and 122 telephone numbers) and systems for person or vehicle tracking.

As a consequence of the development of both location estimation technologies and location based services, location information is more and more used everyday. This novel situation raises several challenges that researchers must face to [1]. One of these challenges lies in the development of solutions to provide end-to-end control of location information. A particular area where it is necessary to research is the development of mechanisms that guarantee user's privacy and location information's trust (authentication and attestation). Moreover, Patterson *et al.* advise that researchers participate in the preliminary steps of the mechanisms development and use, before commercial companies take charge of them.

This work focuses on the problem of digitally certifying the location of an entity at a given time. Our research builds upon the spatial-temporal certification framework developed by González-Tablas, Ramos and Ribagorda [2]. Particularly, our work addresses the implementation of CERTILOC, a prototype of a spatial-temporal certification service following González-Tablas et al. model. We have designed the system to be compatible with several localization methods, to use existing standards when appropriate and to follow a modular design. Besides the value that a real implementation provides, our work contributes also by analyzing the security of this kind of systems from a broader point of view and its legal implications when used for workforce monitoring scenarios.

Related work. During the last decade some spatial-temporal certification models and mechanisms have been proposed in [3, 4], but none of them addresses their implementation besides that they focus on specific application scenarios. On the other hand, [5] presents a proof of concept implementation of a GPS-enabled device which sends its location data protected with a self generated digital signature. This implementation could be integrated in our system as an alternative localization subsystem.

Paper outline. In Section 2 the main concepts of González-Tablas *et al.* spatial-temporal certification framework are described. Section 3 presents the principal features of the implemented spatial-temporal certification service. In Section 4 and 5 discuss the security analysis and legal implications respectively. Finally, Section 6 summarizes the conclusions and lessons learned from our work.

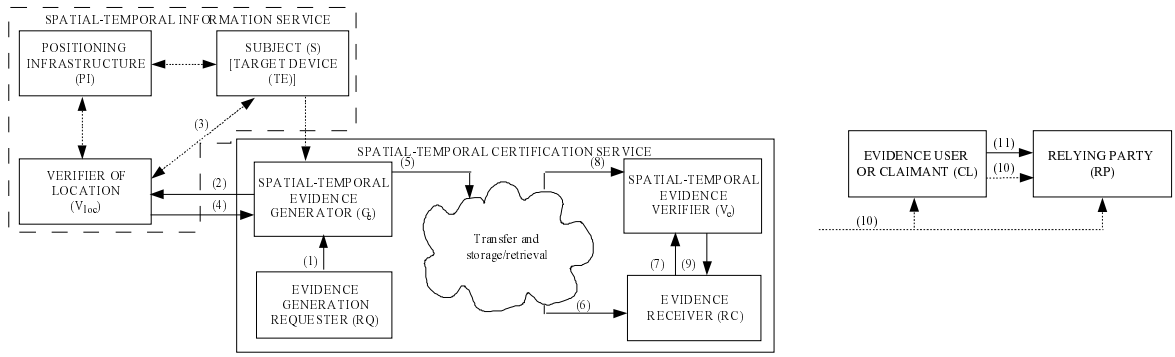
2. Spatial-temporal certification services

Spatial-temporal certification services are defined by González-Tablas *et al.* as *those services that generate, collect, maintain, make available and*

validate evidences concerning the spatial-temporal information of an entity [2]. Therefore, evidences generated by spatial-temporal certification services attest that some entity was located at some place at some moment in time under some specific policy. Such evidence is called Spatial-Temporal Certificate (STC) and it binds certain Spatial-Temporal Information (STI) to some entity.

Spatial-temporal certification services find their application in non-repudiation scenarios, for example, in the tracking of entities and assets such as mobile workers, vehicles, hazardous materials or valuable assets, and in location-based billing such as in automatic toll collection systems either for highway usage or for vehicle stay in certain areas (i.e. preserved environmental zones such as biosphere reserves). STCs can also be used to enforce security policies, for example, an on-line gambling site may require to its clients to be located within some specific geographic area, or a shopping centre may desire to grant privileges depending on users' visiting history.

The provision of spatial-temporal certification services takes place in several phases in which several entities may participate (see Figure 1).



(a) Phases: certificate generation; certificate transfer, storage and retrieval; and certificate verification. (b) Phase: certificate use.

Figure 1. General model of spatial-temporal certification services

First phase is *certificate generation*, in which a requester RQ asks for the generation of a STC for a specific subject S to the spatial-temporal evidence generator G_e. This G_e issues the STC after obtaining the location information of the subject S from a secure Spatial-Temporal Information Service (STIS). STISs act as location servers but in the model it is assumed that the methods they use to obtain the location information guarantee its authenticity to some extent. Second phase considers the *certificate transfer, storage and retrieval*, this way, the STC reaches the intended receiver RC. Third phase is *certificate verification*, which is performed by a spatial-temporal verifier V_e.

Fourth phase comprises the *certificate use*. In this case the evidence user or claimant CL is who makes use of the spatial-temporal evidence to obtain some benefit (e.g. access to some resource or some tax charge). The relying party RP is the entity that provides some benefit to the claimant based on the evidence and maybe other auxiliary information.

The fifth phase, which does not always occur, is *dispute resolution*. If the cited CL and RP do not agree whether some benefit has to be granted, both parties may leave the decision to an adjudicator, who will judge taking into account the available evidences and the policies under which they have been issued.

González-Tablas *et al.* present also a set of requirements on several fundamental aspects of spatial-temporal certification that implementations of these services should fulfill. The addressed aspects are the establishment of trust on the evidences, the policies under which the evidences are issued, the protection of spatial-temporal information privacy and supporting functionalities. Furthermore, two basic STC structures that follow respectively the X.509 attribute certificate framework [6] and the SAML standard [7] are defined. For more details on these issues, we refer the reader to the previous work of González-Tablas *et al.* in [2].

3. Description of the system

The main goal of this work is to implement CERTILOC, a prototype of a spatial-temporal certification service based on the model proposed in [2]. Our system addresses the first three phases described in the model, as the certificate use phase will depend on the application in which the system may be integrated and the fifth phase usually takes place in legal contexts. Gonzalez-Tablas *et al.* model defines a useful baseline framework that must be refined in order

to build a real system. Following we describe the characteristics of our system.

One of the main characteristics of CERTILOC is that it is designed to be compatible with different localization technologies. Currently the prototype obtains the location information from two spatial-temporal information services, one for GSM devices (STIS-GSM) and another one for GPS-enabled devices such as PDAs, smart phones or similar devices (STIS-GPS). Location method in the case of GSM network is Cell-ID. The selection of these two localization subsystems is motivated because they are the most spread location estimation technologies and they are representative of the main current localization methods, network and terminal-based localization respectively.

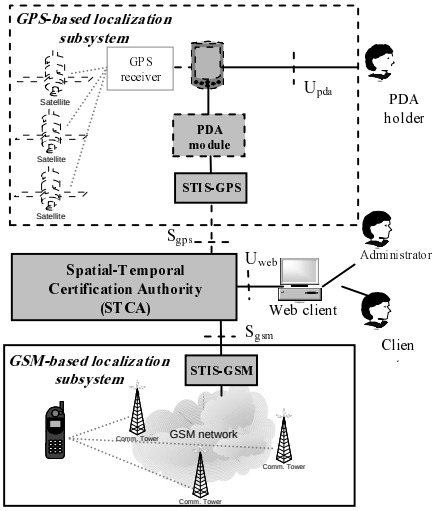


Figure 2. Overview of CERTILOC

The majority of the system's functionalities, grouped in the Spatial-Temporal Certification Authority (STCA), are accessible through a web interface of the logic deployed on the main CERTILOC server (see Figure 2) although there is also some functionality offered through the PDA's interface to the PDA holder. In our system, the receiver of the evidence is the same entity that requested its generation for the sake of simplicity, although it would be straightforward to change the system so both entities differ.

Some remarks have to be made about the design of the GPS-based localization subsystem. Regarding that GPS-enabled devices locate themselves, the PDA module must exist to communicate its location to externals. Additionally, taking advantage of that, we designed this subsystem as a first approach to a distributed spatial-temporal certification service, that is, instead of having a central service issuing all the STC for every subject, self-located devices may issue *self-signed STC* (simplified certificates referring to themselves). For this purpose, the device's software and hardware should be reliable enough.

Besides, STIS-GPS solves, at least from the server's point of view, the limited connectivity problem that PDAs suffer from. The STIS-GSM returns immediately a response to location requests about GSM devices (*immediate requests*). However it cannot be assumed that PDAs will be always accessible to attend to the location requests directed to them. Therefore, our system is designed such that *deferred requests* (those location related requests referring to connection limited devices) are served in three phases: first, requests made by users are stored by the STCA in a database shared with the STIS-GPS; second, as soon as the PDA connects to the STIS-GPS, the pending requests are attended (the STIS-GPS stores self STCs issued by the PDA in the cited database); third, users access a second time to the system to trigger, if possible, the completion of their location or certification request.

Although we plan to integrate in CERTILOC a policy based privacy management and enforcement mechanism, it is still not implemented, but the design already considers this future functionality.

The following sections of this chapter explain both the design and implementation of CERTILOC. Section 3.1 contains its functionalities. Section 3.2 describes its architecture. On section 3.3, the specific technologies in use and implementation details are shown. Finally, Section 3.4 focuses on CERTILOC´s timing performance.

3.1 Functionalities

First of all, the prototype can *locate devices*. A client can access the system through the web interface and make a location request. The system then transfers the request to the appropriate STIS and, when the STI is available, it is transferred to the client. If the located device has limited connectivity, the client gets instead a locator, which allows him to resume his request afterwards if it has been attended.

Furthermore, the system allows clients to *certify devices' location*. The STCA, after having obtained the STI, generates and stores a STC. As in the previous case, if it is a connection limited device, the user gets a locator to resume his request afterwards. The prototype also allows clients to *manage STC´s lifecycle* (download, remove and consult certificates).

Administrators can *administrate users and devices*. They can register new users, unregister them and modify their registration data (an identifier, a client or administrator role, an alternate identifier, an e-mail and

the authentication information). Administrators can also register devices, unregister them and modify their registration data (an identifier and the identifier of its owner, the entity responsible of the device). Moreover, administrators can *consult the activity logs*, where user and system actions are recorded, and to *configure the system* by establishing some basic parameters (STC expiration time, specific storage place for STC, etc.).

The PDA user can *generate voluntary self-signed STCs at any time* through the interface in the PDA. These self STC are afterwards used by the STCA to generate a complete STC. PDA users can also specify some configuration parameters (related to the relationship between the PDA and the STIS-GPS).

Finally, regarding the privacy management and enforcement, it is planned (but not implemented) that any client responsible of a device will be able to upload and remove privacy policies which will specify under which conditions a user would allow the processing of the STI related to devices the user is responsible of.

3.2 System architecture

Figure 3 contains the system's deployment diagram. As seen on the figure, logic is distributed in two nodes (CERTILOC server and a PDA). The main component deployed on CERTILOC server node is the STCA, which follows the MVC architectural pattern and is structured in three layers:

- **Base platform.** This layer contains only one component. It receives user actions and makes callings to the essential services.
- **Essential services.** This layer contains the components in charge of the main functionalities of the prototype.
- **External representatives.** This layer contains the spatial-temporal information providers, which are the components which connect to the STIS. Note that there are two providers, one for immediate requests and another for deferred ones. This layer also contains the component to access the data sources.

Besides the STCA, the entire GSM-based localization subsystem and the GPS-STIS are also deployed in CERTILOC server node. The certificates repository and the database shared between the STIS-GPS and the STCA are also placed in the server node.

3.2.1 Dynamic behavior. Following we will explain the dynamic behavior of CERTILOC according to the two location related requests available through the web interface (*immediate* and *deferred* requests) and to the request for generating voluntary self-signed STC available through the PDA interface. We will identify the main processes that take place in each request. For now on, the term *request* can be interpreted as a *location* request or a *certification* one.

Users can make an **immediate request** after logging in the system through the web interface (*request generation*). The "certification and location" module then calls to the "immediate location provider" (*internal STI retrieving*) who transfers the request to the adequate STIS (STIS-GSM) using Mobile Location Protocol 3.0 [INT06] (*external STI retrieving*). This component should contact with the location network to get back the requested STI, but in our case this process has been emulated. STI is sent back (*STI transference*) to the STCA. The STCA enforces then the privacy policies defined for the located device (*privacy enforcement*) dictating if the rest of the processes may take place. If the request was for certifying the STI, then the *complete STC generation* process is done and the STC is inserted into the database (*database updating*). Finally the result, STI or STC, is transferred to the user (*system response*).

In case of **deferred requests**, when the client makes the request, it is inserted into the database and a locator is sent to the user (*request insertion*). Periodically, the PDA gets securely connected to the STIS-GPS (*device connection*) using Wi-Fi access and a self-defined protocol with mutual authentication built upon HTTP over SSL. The STIS-GPS looks for unanswered requests in the database (*request retrieving*) and if any, they are securely sent to the device (*request transference*). Then, the PDA, which has been registering periodically its own STI, answers each request building a self-signed STC using the closer in time STI known (*request resolution*). Those self-signed STCs are sent to the STIS-GPS (*answering certificate transference*), which validates and inserts them in the database (*answering certificate insertion*). When the client returns to the system and uses the provided locator (*deferred request resuming*), after privacy policies are checked (*privacy enforcement*), the STI or the STC built upon the referred self-signed STC (*complete STC generation*) are sent to the user.

The PDA holder can **generate at any time voluntary self-signed STCs** (certify its own position) which are also used by the STCA to build complete STCs.These STCs are preliminary built when the PDA holder orders the certification (*voluntary STC initial generation*) but their signature is generated when they are sent to the STCA within the cited *certificate transference* process. As a difference with the previous case, the *complete STC generation* is started automatically by the STCA.

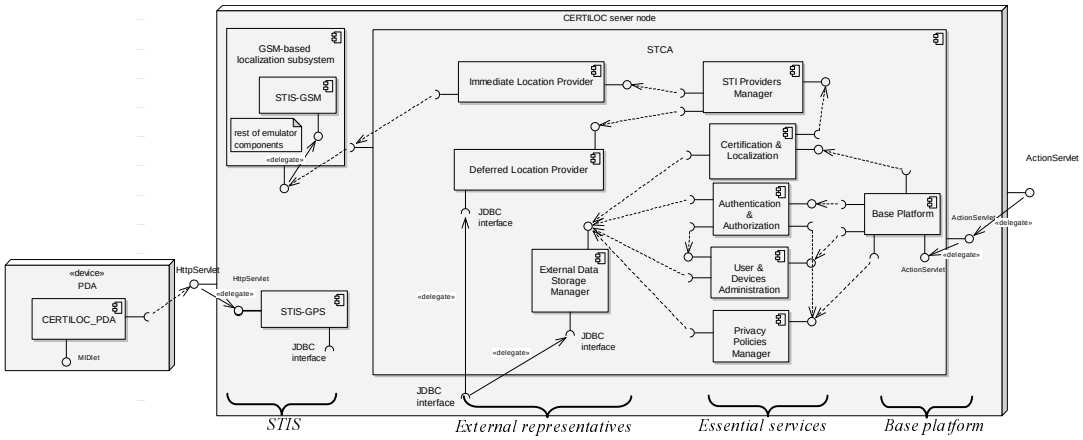


Figure 3. CERTILOC´s deployment diagram.

3.2.2 Security mechanisms. Besides the security mechanisms established in the connections between the STCA and the STISs, user authentication and authorization mechanisms are also integrated in CERTILOC. Regarding user authentication, web interface currently offers a classical user and password access, although the use of X.509 public key certificates is planned. PDA holder authentication is not considered in CERTILOC, because, among other reasons, it would lead to a less friendly mobile application (user should be asked for using his private key for every location request). Regarding user authorization, currently the system only checks if the user´s role (client or administrator) is able to make the request. In next release, if the action involves spatial-temporal information (i.e. locate a device, retrieve a STC, etc.), the system will check if it is allowed by the privacy policies established for the affected device.

3.3 Implementation details

The whole prototype has been implemented using Java (J2EE for server, J2ME for mobile device). Server node is equipped with a dual-core processor, and Ubuntu Linux 6.0.6. Server components are running on several web application servers (Apache Tomcat 5.5.23). The STCA has been implemented using the Struts framework. Related to STC generation, we selected OpenSAML 2.0 [9] (currently under development) and we followed, depending on the facilities provided by the OpenSAML software, the SAML based STC structure defined in [2]. With respect to data storage, MySQL 5.0.5 is used, being accessed through JDBC connectors.

Regarding the GSM-based localization subsystem, it has been emulated using software provided by Ericsson [10]. Regarding the GPS-based localization subsystem, SIET-GPS has been built using Java Servlets and the GPS-enabled device is a N95 model from Nokia which supports J2ME applications over the Symbian O.S. and is compliant with the Java Location API [11] (which allows the obtaining of location data from the GPS receiver). For all cryptographic operations, we use the Bouncycastle API [12].

Finally we have to remark that we have not been able to connect the PDA and the SIET-GPS through a SSL tunnel yet because of the current configuration of our University infrastructure. Nevertheless, this matter will be addressed in a few months.

3.4 System performance

In this section we present the time yield of the system from the user point of view. We have analyzed system performance differentiating the system interoperating with the GSM-based localization subsystem and with the GPS-based one. Table 1 shows the results of time measurements.

Table 1. Results of time measurements.

Time ID	Process	Mean time
GSM-based localization subsystem		
T_1	Location request	3.13 sec.
T_2	Certification request	3.86 sec.
GPS-based localization subsystem		
T_3	From *device connection* to *answering certificate insertion*	13.53 sec.
T_4	*Voluntary STC initial generation*	3.9 sec.
T_5	*Certificate transference* (for voluntary STC)	4.97 sec.

3.4.1 GSM-based localization subsystem. Table 1 shows the mean time in seconds for location (T_1) and certification (T_2) requests related to GSM devices. These results were expected taking into account the complexity of the involved tasks and the available

resources to carry out them. The difference between the two times is due to additional processing is needed for composing the STC in certification requests.

3.4.2 GPS-based localization subsystem. Table 1 shows time measures for the essential processes related to GPS-enabled devices. Process names used in this section are taken from those identified in section 3.2. Note that neither *request insertion* nor *deferred request resuming* processes have been timed, because they were negligible compared to the rest of times.

First of all, time measurement T_3 represents the time between the PDA gets connected with STIS-GPS for obtaining pending requests, and until its responses are correctly stored in the server database. It is reasonable to attribute the high amount of time consumed to the amount of processing and resources employed simultaneously in the PDA.

In case of voluntary self-signed STC, as said on section 3.2, the process is divided into two parts, and each of them has been timed separately. Time measurement T_4 represents the time in the PDA to create the data structure that will be included in the certificate. Although this process involves connecting with the GPS receiver, it is relatively fast (at least, admissible for the user experience). This data structure is stored until the next connection to the STIS-GPS takes place. Time measurement T_5 shows the length of this connection, during which the stored certificate is retrieved, digitally signed and finally sent to the server. As seen on table 1, signing and sending the voluntary self-signed STC is significantly harder than only generating it. Comparing the times obtained for this technology with the previously one, times are larger in case of GPS-enabled devices although essential tasks are the same (creating data structures, making digital signatures and communicating). This result was expected, because PDAs have fewer resources.

4. Security analysis

In this section we analyze the system from a security point of view. Besides all security requirements that are shared by every connected system (availability, correct user identification, authorized users access, etc.), in this kind of systems it is essential to assure that STI (and also the certificates derived from it) is protected against tampering and unauthorized access. We will use Figure 4 to help in the analysis.

First threat that CERTILOC, and systems of its kind, must face to is *identity spoofing*. In CERTILOC web users access the system through the channel marked as EC_1 and they are forced to log into the system either with user and password or, in the future, with their public key certificates. Once authenticated, user actions take place inside a session whose correctness is checked in every request, avoiding then the occurrence of *privilege escalation attacks*.

An attacker may try also to impersonate the STCA in order to access the GSM-based localization subsystem (e.g. to know the location of certain device without being authorized), but this threat is mitigated by the user/password authentication mechanism required by the Ericsson MPS SDK software. In our system, the GSM network including the mobile phones is emulated, so there is no point in analyzing identity spoofing threat between these entities. However, an implementation interoperating with the real GSM network should seriously consider it.

An attacker may also try to impersonate the STCA or the STIS-GPS in order to access the shared database between them or the STCs database. In CERTILOC this threat is again reduced by requiring user/password authentication to access the mentioned databases.

An identity spoofing attack could also be performed for both the PDA and STIS-GPS, one against each other, in channel EC_2. This could allow to obtain the STI unauthorized (if STIS-GPS identity is spoofed), or to provide fake STI (in case of PDA spoofing). For this purpose, an SSL tunnel with server authentication is established. Client (the PDA) authentication is made within our self-designed communication protocol.

Another threat that must be considered specially in this kind of systems is *location spoofing* (i.e. modifications over the STI). Essentially, this threat could take place wherever any STI is involved. Satellite signals (EC_4) could be intentionally altered or substituted, and this cannot be mitigated (at least, with public GPS technology). Furthermore, the PDA could be manipulated, which could be avoided by using tamper-resistant hardware. Besides, the transferred STI from the PDA could also be altered within the communication (EC_2). In our case, additionally to the cited SSL tunnel (which could be enough), the digital signature made for certifying the information also guarantees its integrity. This digital signature is also the mechanism established to alleviate this threat in the databases placed in the server node, although it would be advisable to analyze the data introduced by users through the web interface (which could lead to SQL injection attacks). It is important to remark that in a real GSM-based localization subsystem it would be also necessary to take measures against this threat.

Other threat to take into account is the *loss of privacy*. This could be achieved in two ways. First, an attacker could try to access to confidential data. In our

system, this could be attempted in all databases and in EC_1 and EC_2 channels. To reduce this threat in our system, all accesses to this data are previously authenticated. Furthermore, the server node is equipped with a software firewall and it is placed inside a safely designed LAN. In case of the data stored into the PDA, it has been protected by using only internal memory. Nevertheless, it would be desirable to cipher all data storages.

The second way to achieve loss of privacy could be derived from an unauthorized use of the obtained STI (regarding that STI is considered a private data when referred to a person). To ease this threat, security policies enforcement and management mechanisms are planned for future releases.

The last kind of threat considered is *denial of service*. This could be attempted on PDA (by sending a great couple of location requests), on satellite signals (by jamming attacks) or on the server node (by making lots of simultaneous requests). Among all of them, the only prevented in CERTILOC is the attack over the PDA, because the operating system takes care about resources consumption.

Including all of the referred measures would not lead to a completely safe architecture, but to a reasonably defended system against external threats. Nevertheless, it would be possible to perform insider attacks (i.e. complete deletion of database by an administrator, perhaps accidentally). These attacks are managed in three ways in our system: avoiding their occurrence (by reducing the amount of user actions of each role in the system), preventing accidents (by following usability guides) and finally recording them (into a system log). All these measures should be backboned by an appropriate security management plan (i.e. backups, restricted system access, password changing, etc.), but this is not achieved in this work.

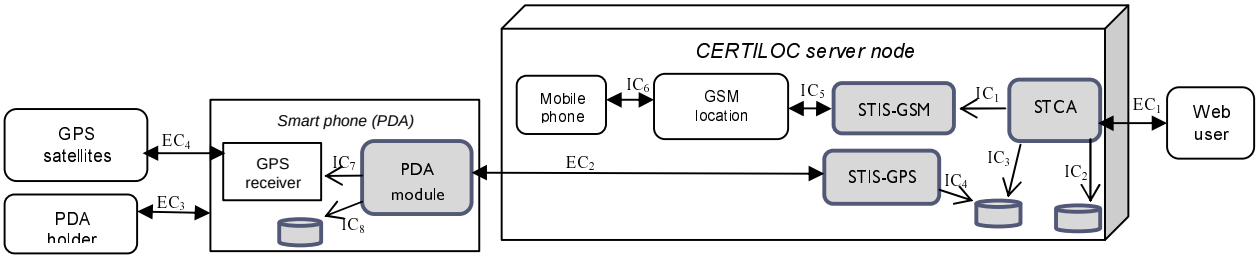


Figure 4. Security analysis scheme

5. Legal issues in workforce monitoring scenarios

The system we have implemented has as main goal to certificate the STI of some devices. In this section we analyze firstly the authority of an employer to monitor an employee using the system and secondly the legal validity of the STC once generated.

It has to be remarked that when a device is directly or potentially related to someone, its STI is also its holder´s one. This fact is especially relevant from the legal point of view, because the location information of a person is considered as personal data, and therefore it must be protected (as dictated by [13], transposed in Spain in [14]). One of the applications of this prototype would be to integrate it in a working scenario, that is, as surveillance or control measure. It is then very important to assure that this use of our system is in compliance with legislation. The following considerations address this issue considering the Spanish law, but they can be easily applied to any European country belonging to the European Union as they all have as base the same European Directive [13].

In the Spanish workers statute [15], it is stated that the employer can give to the employees devices that can be located as a tool of working. Nevertheless, if the employer collected the location data of his employees (personal data, from the legal point of view), he should inform them about this collection [14]. Employees would not be required to allow this action, but they have to consider that this collection is probably made to preserve and accomplish a previously existent contractual relationship.

Once the employer has the right to obtain the employees' STI, he could take decisions based on it. He could punish or even fire an employee for not being in the place he was assumed to be, although this action could be resorted in legal courts [15]. In this situation, the point of interest is to analyze the legal value of STC as evidence within a judiciary process. The STC is a digitally signed electronic document, and so it can be used as evidence [16]. Nevertheless, its validity is conditioned to the strength of the digital signature. The digital signature now made by the prototype may be considered as an "*advanced digital signature*" [17]. This kind of signature is not enough to have the same validity as a handwritten one. To achieve this, in

addition to the saying until now, the whole prototype should be checked as a "*secure signing device*". This condition should be fulfilled by real systems based on this prototype, in order to assure the credibility as an evidence of the generated STC.

6. Conclusions

The fact that nowadays location information is more and more used promotes researchers to address the challenges that arise for guaranteeing an end-to-end control of this information. The system we have implemented addresses the implementation of a prototype of a spatial-temporal certification service that is based on the model proposed in [2] and is compatible with two localization technologies, GSM Cell-ID and GPS. This kind of practical research has not been commonly addressed, which gives a special value to our work.

Our work is not only an implemented prototype, but also a system whose design has focused on dependability issues. In the system there is a modular division of responsibilities and commonly accepted standards are in use, which make the prototype more flexible. The dependability is also reflected in the integrated security mechanisms, which do not lead to a complete safe architecture but to a reasonably defended system. Furthermore, we analyze also the legal implications of using the system in work scenarios.

Though the prototype is completely functional, we are currently working in the development of a policy-based privacy management and enforcement module and in extending the prototype to locate RFID labels.

The main lesson learned from our work is that it is viable to implement this kind of systems although they have to deal with a great number of complex security threats, some of which can be easily mitigated but others are difficult to prevent. Another issue is that commercial mobile devices may not have still enough resources to address adequately the security requirements.

Acknowledgements

The authors would like to thank José Carlos Calvo Martínez for collaborating in the implementation of the system. Authors are partly supported by "Dirección General de Investigación del M.E.C. (SPAIN)" under contract SEG2004-02604.

References

[1] C. A. Patterson, R. R. Muntz, and C. M. Pancake, "Challenges in location-aware computing", *IEEE Pervasive Computing*, 2(2):80–89, April 2003.

[2] González-Tablas, A.I, Ramos, B., Ribagorda, A., "Spatial-temporal certification framework and extension of X.509 attribute certificate framework and SAML standard to support spatial-temporal certificates", in Proc. of EuroPKI'07, 2007.

[3] L. Bussard. Trust Establishment Protocols for Communicating Devices. PhD thesis, Institut Eurécom, Télécom Paris, 2004.

[4] A. Zugenmaier, M. Kreutzer, and M. Kabatnik, "Enhancing applications with approved location stamps", in Proc. of IEEE Intelligent Network Workshop, 2001.

[5] Wullems, C.; Pozzobon, O. and Kubik, K., "Trust your receiver? Enhancing location security", *GPS World*, 2004, 15, 23-30.

[6] ITU-T. ITU-T RECOMMENDATION X.509 - Information technology – Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, August 2005.

[7] OASIS. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) Version 2.0. OASIS Standard, 2005.

[8] Open Mobile Alliance, *Mobile Location Protocol (MLP) – Version 3.0*, June 2002.

[9] Internet2, OpenSAML 2.0, October 2006

[10] Ericsson, MPS SDK 6.0.1, March 2004.

[11] Sun Microsystems, *Java Specification Request 179*, March 2006

[12] Legion of the Bouncy Castle, Bouncy Castle Crypto API version 1.3.7.

[13] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, July 2002.

[14] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, Spain, 1999.

[15] Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, Spain, 1995

[16] Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, Spain, 2000.

[17] Ley 59/2003, de 19 de diciembre, de firma electrónica, Spain, 1999.