Providing personalization and automation to spatial-temporal stamping services

A. I. González-Tablas, L. M. Salas, B. Ramos and A. Ribagorda
Grupo de Seguridad en las Tecnologías de la Información y las Comunicaciones (STIC)
Departamento de Informática. Universidad Carlos III de Madrid. Leganés, Spain - 28911
Email: aigonzal@inf.uc3m.es, luismisg@terra.es, benja1@inf.uc3m.es, arturo@inf.uc3m.es

Abstract

We describe a policy model and a language designed to provide personalization and automation to spatial-temporal stamping services. These security services have been recently proposed in the context of location based services. Their goal is to issue non-repudiation digital evidences about the spatial-temporal conditions of mobile entities. One of the issues that existing spatial-temporal stamping services have not addressed is how to incorporate personalization and automation in the stamping. We propose an enhanced spatial-temporal stamping service which fulfills these requirements by integrating a policy framework. In this paper we focus on the information model and the policy language. Our language, defined using XML schema, allows a personalized specification of the spatial-temporal conditions that trigger automated spatial-temporal stamp requests.

1. Introduction

The development of positioning technologies and the increasing mobility of our communications have allowed the deployment of Location Based Services (LBS) [21]. LBS offer value-added services based on the geographic position of mobile devices. Between its applications the following ones stand out: emergency, security and medical services; information and navigation services; m-commerce, toll collecting and billing systems; resource tracking and fleet management; and entertainment and proximity services [7].

In the context of LBS applied to m-commerce and m-administration, there are some applications that will benefit of authenticating the location of certain entity. *Location authentication protocols*, such as the ones proposed in [2–4], provide this kind of authentication. In other cases, an evidence about the spatial-temporal conditions of certain entity is what is needed. *Spatial-temporal stamping services*, which some authors call *location stamping services*, provide this kind of digital evidences. These evidences are issued by trusted entities and can be verified afterwards by third parties. Some spatial-temporal stamping services have been proposed in [1, 8, 23]. Location authentication protocols and spatial-temporal stamping services allow, for example, the following applications:

- Enforce access control based on current or past location-time conditions, or in its history.
- Implement notarization functions that include location information.
- Track entities, such as valuable assets, mobile workers, nodes in a network, hazardous material, etc.

Some applications, such as tracking applications, will benefit if personalized and automated spatial-temporal stamping is provided. Users' trust and confidence in spatial-temporal stamping services (and therefore in LBS that use them) will increase if they can personalize the stamping. Automating the stamping according to some conditions will facilitate service provision and management, while decreasing user disturbance. How to incorporate these characteristics in spatial-temporal stamping services has not been addressed yet.

The following example scenarios illustrate some applications that benefit if automation and personalization of the stamping is provided. One scenario considers a goods transport company in which the trucks and its drivers are tracked. The company may want that a spatial-temporal stamp is issued every 30 minutes or if the truck is following some predefined route. The company may even want to make sure about the driver being close to his designated truck during the whole route including the rest intervals. This would prevent the drivers to skip their forced rest to drive more hours.

In another scenario it is considered a company who offers its services in a closed big area, such as an amusement park. This company may offer discounts or advantages to users that visit its site with some frequency. If a spatial-temporal stamp is requested automatically each time the user visits the area, these stamps can be shown later to the company to get the promised benefits, but at the same time

the company has been prevented to know the user whereabouts until the user decides it.

In this paper we propose a spatial-temporal stamping service which integrates a policy framework to provide automation and personalization to the stamping. Policies have been defined as the '*rules that govern the choices in behaviour of a system*' [20]. They are one of the most used mechanisms to implement flexible and adaptable management functions for Internet, distributed services and security systems. A policy-based management system enforces a specific behaviour in a system by interpreting a certain policy. Policy-based management implies to consider how to specify the policies (information model and policy specification language) and the policy deployment architecture (policy distribution and enforcement). In this paper we focus on the information model and the policy specification language. Our policy framework is based in XACML, Ponder and IETF/DMTF policy frameworks [5, 15, 18], and our policy specification language is defined using XML schema [22]. It allows a personalized specification of the spatial-temporal conditions which trigger automated spatial-temporal stamp requests or other actions.

The rest of the paper is organized as follows. First the description of spatial-temporal stamping services and the assumptions made on their general model are presented in Section 2. In Section 3 we explain our proposal to integrate a policy framework in spatial-temporal stamping services. Section 4 demonstrates the application of the framework by presenting some examples. Section 5 is devoted to analyzing some related works and, finally, Section 6 summarizes some conclusions and open issues.

2. Spatial-Temporal Stamping Services

We define *spatial-temporal stamping services* as those non-repudiation services that collect, issue, maintain, make available and validate evidences about the spatial-temporal conditions of certain entities. In the previous definition, evidence means the *'information that either by itself, or in conjunction with other information, is used to establish proof about an event or action'* [10]. In this case, the event or action refers to certain entity (subject of the evidence) being at some position (geographic or symbolic) at certain time.

Several entities may be involved in the provision of spatial-temporal stamping services (see Figure 1): The *Spatial-Temporal Stamping Authority* (STSA) is the trusted third party that issues the evidences or spatial-temporal stamps. The entity which the stamps refer to is the *Subject* (S) of the evidence, which includes a *Subject Device* (SD) and optionally a *Final Subject* (FS). Subject devices are those that can be located with current positioning technology; final subjects are those entities who control them.

Positioning technologies can be divided in network-based and terminal-based depending on which entity computes the device location. Spatial-temporal stamping services can rely in both positioning technologies, but in this paper we will only consider network-based. Under this restriction, we define *Spatial-Temporal Information Services* (STIS) as the entities that provide the position at certain time of at least the subject device and sometimes also of the final subject. *STIS* are the external interface offered by network infrastructures with positioning technology to third parties (usually called LoCation Servers or LCS). The *Mobile Location Protocol* (MLP) standard defines a common interface for wireless networks independent of the underlying positioning technology [12].

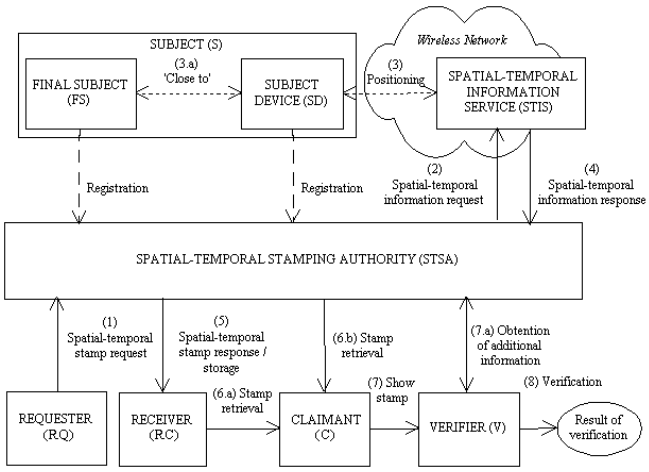

Figure 1. General model for spatial-temporal stamping services

The users of a spatial-temporal stamping service include the following ones: *Requester* (RQ), who requests a spatial-temporal stamp; *Receiver* (RC), which obtains a spatial-temporal stamp after it has been issued; *Claimant* (C) or prover, who wants to prove the validity of a spatial-temporal stamp to some verifier; and *Verifier* (V), which proves the validity of the digital evidence using if necessary information not included in it. Depending on the scenario, one entity may assume several of these roles, for example, the requester may be also the final entity of the evidence.

Spatial-temporal stamping services comprise three main phases as non-repudiation services do [10] (see Figure 1 for the numbers in brackets):

- *Evidence generation.* In this phase, the requester asks the *STSA* for a spatial-temporal stamp on certain subject indicating also the intended receiver (1). The *STSA* verifies the request and then asks the *STIS* for the location information related to the subject at that moment (2). The *STIS* locates the subject (3) and returns to the

STSA this information (4). Finally, the *STSA* generates the spatial-temporal stamp.

- *Evidence transfer, storage and retrieval*. In this phase, the spatial-temporal stamp is transferred to the indicated recipient or stored in some repository (5). Later on, the spatial-temporal stamp is retrieved by or transferred to the claimant (6).
- *Evidence verification*. In this phase, the claimant shows the spatial-temporal stamp to the verifier (7), who verifies its correctness and validity (8).

The spatial-temporal stamp generation mechanism is typically a digital signature on at least the following data: a unique serial number, the subject identification, the spatial-temporal information including the resolution, and the identifications of the *STSA* and the *STIS* which collaborate to generate the evidence. This structure resembles some of the existing attribute certificates [14, 19]. In fact, spatial-temporal stamps may be defined as attribute certificates (being the attribute the spatial-temporal information) when used in authorization scenarios. The stamp verification consists in verifying the correctness and validity of the signature, using the appropriate verification key and other necessary information such as certificate revocation lists.

In most application scenarios, it is probable that the requester, the receiver and the claimant are the same entity who wants to prove its spatial-temporal condition to the verifier in order to get access to some service or avoiding some penalty. In notarization scenarios, the requester and receiver may be the same entity different than the subject of the evidence. For example, an electronic shop that applies distinct prices depending on spatial-temporal conditions and afterwards must justify its sales to another entity.

We make some assumptions in this model. First, subject devices must have communicating capabilities which allow their positioning by the wireless network infrastructure which the *STIS* belongs to. Sometimes these capabilities may extend to positioning the final subject close to the subject device (as proposed in [11]). It is also assumed that subject entities have registered with the *STSA* and also with the *STIS* for this service. Users trust *STIS* to locate subjects in a secure and correct manner and *STSA* to generate the spatial-temporal evidences. Finally, the entities can authenticate each other and carry out secure communications using mechanisms that are not addressed in this paper.

Although privacy is a very important issue when personal information, such as location, is obtained and used, it is not addressed in this paper. This work is part of a bigger project[1] which will further investigate how to integrate privacy issues in spatial-temporal stamping services.

[1]Contract SEG2004-02604 with 'Dirección General de Investigación del Ministerio de Educación y Ciencia': *'CERTILOC: Digital CERTIfication service for LOCation information'*

3. Integration of a Policy Framework in Spatial-Temporal Stamping Services

3.1. General Description and Assumptions

From our point of view, *spatial-temporal stamping policies* define a set of spatial-temporal stamping rules (obligation policies) for some subjects. Each rule considers a spatial-temporal condition, the events that trigger its evaluation, and the actions that must be performed if it evaluates to true. For example, a spatial-temporal stamping rule may define that a spatial-temporal stamp must be requested if a subject entity is at certain place within certain time interval.

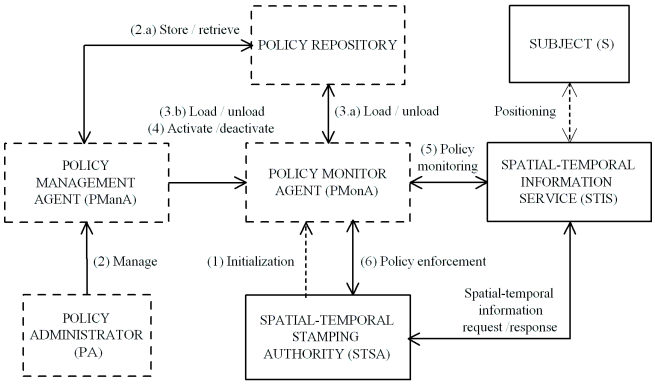

Figure 2. Integration of a policy framework in the model

Our proposed spatial-temporal stamping model with an integrated policy framework is depicted in Figure 2. We have considered the same entities of the IETF/DMTF policy framework [17], but the original Policy Decision Point (PDP) and Policy Enforcement Point (PEP) are merged in one entity, the policy monitor agent. We assume that the incorporated entities can also authenticate each other and other entities, and carry out secure communications. Although our policy framework is presented as part of the spatial-temporal stamping service, in some scenarios it could interesting to consider it as a separate service.

The *Policy Management Agent* (PManA) allows the *Policy Administrator* (PA) to manage spatial-temporal stamping policies (2). Possible actions with policies include the following: creation/deletion, edition, storage/retrieval in/from a *Policy Repository* (2.a), loading/unloading into the policy monitor agent (3) and activation/deactivation once loaded (4). The policy administrator may be the final subject, the subject device's owner or an authorized external entity.

The *Policy Monitor Agent* (PMonA) retrieves the policies from the policy repository (3.a) or receives them from

the policy management agent (3.b). Then the policy administrator activates a set of policies using the *PManA* (4). The *PMonA* enforces the activated policies after processing them to detect which rules are applicable and which events must be aware of to evaluate each rule. For the moment, our framework only considers the *PMonA*'s behaviour adaptation through the assignment of certain spatial-temporal policies by the *PA*. This adaptation is static in the sense that it is determined by the policies and the spatial-temporal conditions of the subject. It would be desirable that, in future developments, the applied policies do depend on the behaviour of entities such as the *PMonA* or the subject, or on network/service characteristics including trust and security.

3.2. Information Model

The proposed information model to represent spatial-temporal stamping policies is shown in Figure 3. Its main elements are `Policy`, `BasicPolicy` and `StampingRule`.

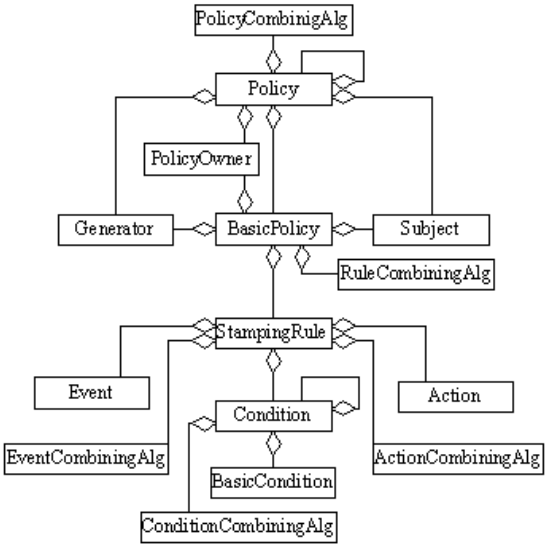

Figure 3. Information model to represent spatial-temporal stamping policies

`Policy` elements allow to group policies and they contain a set of `BasicPolicy` and `Policy` elements combined by a `PolicyCombiningAlg`orithm.

`BasicPolicy` is the basic element that may be loaded or activated by the *PManA* in the *PMonA*. It comprises a set of `StampingRules` elements combined by a `RuleCombinigAlg`orithm such as the `First-applicable` or `All-applicable`. `Subject`, `Generator` and `PolicyOwner` elements are also children of `BasicPolicy` elements. These elements may be absent from a `BasicPolicy` element if this element is a child of a `Policy` element. In this case, they are inherited.

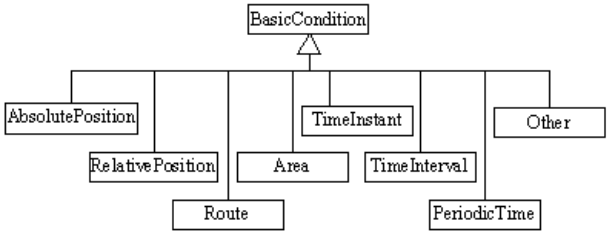

Figure 4. Defined `BasicCondition` types

- The `Subject` element specifies the subject devices and optionally the final subjects of the spatial-temporal stamp requests triggered by the `StampingRules` belonging to its `BasicPolicy` or `Policy` parent.
- The `Generator` element specifies the *STIS* that should provide the spatial-temporal information about the subject and the *STSA* which has to generate the spatial-temporal stamps.
- The `PolicyOwner` is the entity who owns the policy and it is more related to privacy issues.
- `StampingRule` elements determine a single spatial-temporal stamping rule that binds a set of events (`Event`) with a condition (`Condition`) and a set of actions (`Action`).
  - We have not defined specific `Event` types yet, but we foresee that most of them are going to be time-related (such as internal timers notifying a periodic time or some specific time instant), or location-related (e.g. an external event notifying that the subject has entered or left an area, or the reception of periodic location reports). Location-, device- and network-related events are likely to be highly dependent on the specific services offered by the *STIS*. The set of `Event` elements can be combined by an `EventCombiningAlg`orithm, such as `AND`, `OR` and `Sequence`.
  - The `Condition` child allows the specification of a composite spatial-temporal condition using a combination of `BasicCondition` and `Condition` elements. The considered `ConditionCombiningAlg`orithms are `OR`, `AND` and `NOT`. We defined several

`BasicCondition` spatial-temporal types (see Figure 4), although the model allows its extension:

  * `AbsolutePosition` (spatial condition): determined by a point (a set of coordinates in a Coordinate Reference System), and the accuracy considered around it.
  * `RelativePosition` (spatial condition): determined by a reference point, the directed displacement applied from it and the accuracy considered around the relative position.
  * `Route` (spatial condition): determined by an ordered set of points, the linear interpolation between them and the accuracy considered around the whole route.
  * `Area` (spatial condition): determined by a geographic surface contained inside a closed linear segment.
  * `TimeInstant` (temporal condition): determined by a position in time.
  * `TimeInterval` (temporal condition): determined by a time interval specified by two time instants (begin and end of the interval), and optionally the interval duration.
  * `PeriodicTime` (temporal condition): determined by a set of periodic time instants specified by a period duration and two time instants (start and stop of the time interval in which the period is applied).

- Possible `Actions` are to request some specific kind of spatial-temporal stamp, log the triggered rule and raise some event. The set of `Actions` can also be combined by an `ActionCombiningAlg`orithm, typically a `Sequence` algorithm.

Although our information model is inspired by part of the Ponder information model [5], we decided to define our own information model to allow an easier detection and incorporation of new characteristics or requirements specific to spatial-temporal stamping applications. Therefore, most of our elements are also present in the Ponder model but we refined some of them to adapt them to our scenario (mainly `Subject`, `Generator` and `BasicCondition`). Other elements, such as `Event` and `Action` should be also refined and adapted.

At the moment, policy conflict is not possible as we do not allow negative or refrain actions. However, this issue should be considered when the policy framework be extended to integrate privacy policies in the context of the CERTILOC project.

3.3. Policy Language

We have defined a spatial-temporal stamping policy specification language using XML schema [22]. The language implements the information model described in the previous section but it is not presented in the paper because of space restrictions.

The policies defined using our low-level language would be ready to be enforced by the *PMonA*. Besides the advantages provided by the use of an XML technology, taking this decision allows us to use the *Geographic Markup Language* (GML) defined by the Open GIS Consortium [16]. The main goal of GML is to provide a variety of objects that allow the modelling, transport, and storage of geographic information. Furthermore, using XML to specify spatial-temporal stamping policies facilitates the future integration of our specification language with other XML-based languages devoted to access control (such as XACML [15]) or to the definition of location privacy preferences (such as the ones used in GEOPRIV [9] or LocServ [13]).

Anyway, we do not discard to specify first the policies using another high-level language (such as Ponder) and then compile them to our XML language before they are stored in the repository. It would be also desirable that the *PManA* offer a guided and customized policy specification depending on which services are provided by the considered *STIS*s and *STSA*s.

3.4. Policy Deployment and Prototype Implementation

Before the policies can be distributed, the *PMonA* must be initialized for each subject. This is done after a subject has registered to the service and a policy administrator wants to load at least one policy for that subject. A central repository contains the policies that can be distributed using the *PManA*. If the subject device has enough capabilities, the *PMonA* could be executed in it (as a certified trusted code); otherwise, it can be executed in a server.

For the policy enforcement, first the *PMonA* has to process the loaded policies. We foresee this process as the policy analysis to extract a list of low-level rules which include the `StampingRule` information (events, condition and actions), the policy identification, the specific subject and generators, etc. The *PMonA* can also validate the events it must be aware of as part of the process. Once the *PMonA* has processed the policies, it is ready to enforce them if they are activated. When an event that triggers a `StampingRule` is received, the *PMonA* evaluates the rule. If the result is true, it performs the indicated actions.

We are currently implementing a prototype of the system in Java. To emulate the *STIS* we are using the Ericsson's Mobile Positioning System (MPS) Software Development

Kit [6]. As the MPS SDK returns the subject location specified by sectors instead of geographic points, we are being forced to define algorithms that allow the evaluation of the spatial condition against this information.

4. Application Examples

In this section we present two simple examples that illustrate the use of the proposed spatial-temporal stamping language. The first example (see Figure 5) shows a single `StampingRule` containing a single `Event`, no `Condition`, and a single `Action`. The `StampingRule` determines that every 30 minutes during a whole month, an independent spatial-temporal stamp must be requested.

```
<StampingRule StampingRuleId='STSR2'>
  <Event><PeriodicTimeEvent>
    <StartTime> 2005-10-25T13:20:20 </StartTime>
    <StopTime> 2005-11-25T13:20:20 </StopTime>
    <Period unit='minute'> 30 </Period>
  </PeriodicTimeEvent></Event>
  <Action ActionId='urn:certiloc:action:IndependentSTS'/>
</StampingRule>
```

Figure 5. Single `StampingRule` example

The second example (see Figure 6) presents a `BasicPolicy` which specifies the `Subject`, the `Generator` and a `StampingRule`. The `StampingRule` contains an `Event`, a composite `Condition` and a single `Action`. The rule is triggered when the subject enters in the indicated area (a surface determined by three coordinates). An independent spatial-temporal stamp should be requested every 30 minutes while the subject stays within the same area.

5. Related Work

Providing location stamps concerning a mobile entity was proposed independently by Zugenmaier, Kabatnik and Kreutzer in [11, 23], and by the former Kent Ridge Digital Labs in [1]. Their proposals fit in the description presented in Section 2 excluding that Kent Ridge Digital Labs proposal considers also terminal-based positioning devices and that Zugenmaier, Kabatnik and Kreutzer describe some privacy mechanisms. None of them address personalization and automation of the stamping.

González-Tablas, Ramos and Ribagorda proposed in [8] a new kind of spatial-temporal stamp (*path-stamp*) which considers the history of the spatial-temporal conditions of an entity. In their work they pointed out the integration of a policy framework into the spatial-temporal stamping service as a mean to issue the path-stamps, but they didn't describe how this policy framework was designed or the path-stamp policies specified.

```
<BasicPolicy BasicPolicyId='BasicPolicy1' ... >
<Description> My Basic Policy </Description>
  <Subject> <SubjectDevice>
    <EntityId> My mobile phone </EntityId>
  </SubjectDevice> </Subject>
  <Generator>
    <SpatialTemporalInformationService>
      <EntityId> Movistar:Localizame </EntityId>
    </SpatialTemporalInformationService>
    <SpatialTemporalStampingAuthority>
      <EntityId> http://.../certiloc </EntityId>
    </SpatialTemporalStampingAuthority>
  </Generator>
  <RuleCombiningAlgId  CombiningAlgId=
  "urn:certiloc:rule:alg:All-applicable"/ >
  <StampingRule StampingRuleId='STSR1'>
    <Event EventId='urn:certiloc:event:enterInArea'>
      <AreaEvent> <Polygon> <gml:exterior>
        <gml:LinearRing> <gml:coordinates>
        40.3308N 3.7690W,40.3325N 3.7678W,40.3315N 3.7673W
        </gml:coordinates> </gml:LinearRing>
      </gml:exterior> </Polygon> </AreaEvent>
    </Event>
    <Condition>
      <ConditionCombiningAlg
      CombiningAlgId='urn:certiloc:condition:alg:and'/ >
      <BasicCondition> <PeriodicTimeCondition>
        <Period unit='minute'> 30 </Period>
      </PeriodicTimeCondition> </BasicCondition>
      <BasicCondition> <AreaCondition>
        <Polygon> <gml:exterior>
        <gml:LinearRing> <gml:coordinates>
        40.3308N 3.7690W,40.3325N 3.7678W,40.3315N 3.7673W
        </gml:coordinates> </gml:LinearRing>
        </gml:exterior> </Polygon>
      </AreaCondition> </BasicCondition>
    </Condition>
    <Action ActionId='urn:certiloc:action:IndependentSTS'/>
  </StampingRule>... </BasicPolicy>
```

Figure 6. `BasicPolicy` example

Other researchers propose to incorporate policy frameworks in LBSs but they are mainly intended for protecting users privacy. The work done within the IETF GEOPRIV WG [9] or the proposal in [13] are examples of this.

Two high quality policy frameworks that have inspired our work are XACML [15] and Ponder [5]. XACML defines an XML schema for an extensible access control policy language. Unfortunately, their model is only intended for access control and do not consider obligation policies separately from authorization ones. We do not discard to use it later to specify stamp access control policies.

Ponder is an object-oriented, declarative language for specifying management and security policies. The main reasons that made us to discard it are twofold. First, we preferred to define an XML-based language to ease the policy enforcement and its integration with GML and, in the future, with XACML or GEOPRIV frameworks. Second, Ponder is a complex and multipurpose policy specification

language, but it was not developed specifically for context-aware applications. We think that not being constrained by an existing policy language or framework helps to understand the specific requirements of spatial-temporal stamping services and to design a policy framework better adapted to this scenario. Anyway, we think it is a good option to use it in our framework as a high-level policy language that afterwards is compiled to our XML language.

6. Conclusions and Open Issues

After describing a general model for spatial-temporal stamping services, we have proposed an enhanced spatial-temporal stamping service with an integrated policy framework that allows a personalized and automated stamping. The information model on which the policy framework is based has been presented and the XML schema language that implements it has been used in some examples. The preliminar deployment architecture and current prototype implementation have also been described.

Although our proposal is restricted to work with network-based positioning devices, our spatial-temporal stamping model can be applied with some modifications to rely on terminal-based positioning technologies. In this case the *STIS*, the *PMonA* and probably the *STSA* would be placed in the subject device. This issue will be addressed within the CERTILOC project.

As this is an on-going work, some other open issues are left. The framework should be polished as the prototype implementation is developed. In the context of CERTILOC project, privacy issues will be also integrated in the model. Finally, the communications costs introduced by the framework should be evaluated against the users benefits or the savings its use produces, and its security analyzed.

7. Acknowledgment

The authors would like to thank the anonymous referees for their useful comments and suggestions.

This work is supported by "Dirección General de Investigación del M.E.C." under contract SEG2004-02604.

References

[1] L. Anantharaman, V. Singh, F. Bao, and K. P. Prabhu. Method for certifying location stamping for wireless transactions. Patent Number: WO03007542. Publication date: 2003-01-23, 2001.

[2] S. Brands and D. Chaum. Distance-bounding protocols. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pages 344–359. Springer-Verlag New York, Inc., 1994.

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

[4] S. Capkun, L. Buttyán, and J. P. Hubaux. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In *1st ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN 2003)*, October 31, 2003.

[5] N. Damianou. *A Policy Framework for Management of Distributed Systems*. PhD thesis, Imperial College of Science, Technology and Medicine University of London, Department of Computing, 2002.

[6] Ericsson. MPS SDK 6.0.1, 2004.

[7] G. M. Giaglis, P. Kourouthanassis, and A. Tsamakos. *Towards a classification framework for mobile location services*, pages 67–85. Idea Group Publishing, 2003.

[8] A. I. González-Tablas, B. Ramos, and A. Ribagorda. PathStamps: A proposal for enhancing the security of location tracking applications. In *Ubiquitous Mobile Information and Collaboration Systems Workshop (UMICS03). CAiSE'03 Workshops Proceedings*, June 2003.

[9] IETF Geographic Location/Privacy WG (geopriv). Charter, 2003.

[10] ISO/IEC 13888-1. Information technology - Security techniques - Non-repudiation - Part 1: General, 2004.

[11] M. Kabatnik and A. Zugenmaier. Location stamps for digital signature: A new service for mobile telephone networks. In *Networking - ICN 2001, First International Conference*, LNCS 2094. Springer, 2001.

[12] LIF (Location Interoperatibility Forum). LIF TS 101 Mobile Location Protocol Specification, version 3.0.0, June 2002.

[13] G. Myles, A. Perrig, and N. Davies. Preserving privacy in environments with location-based applications. *IEEE Pervasive Computing*, 2(1), 2003.

[14] OASIS. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, 15 March 2005.

[15] OASIS. eXtensible Access Control Markup Language (XACML) Version 1.0 3. OASIS Standard, 18 February 2003.

[16] OGC (Open GIS Consortium). Geographic Markup Language (GML3.0), 2003.

[17] RFC 2753. Framework for Policy-based Admission Control (RFC 2753), 2000.

[18] RFC 3060. Policy Core Information Model – Version 1 Specification, 2001.

[19] RFC 3281. An Internet Attribute Certificate Profile for Authorization, 2002.

[20] M. S. Sloman. Policy driven management for distributed systems. *Journal of Network and Systems Management*, 2(4):333–360, 1994.

[21] A. Tsalgatidou, J. Veijalainen, J. Markkula, A. Katasonov, and S. Hadjiefthymiades. Mobile E-Commerce and Location-Based Services: Technology and Requirements. In *ScanGIS'2003*, 4-6 June 2003.

[22] W3C (World Wide Web Consortium). XML Schema. Part 1: Structures. Part 2: Datatypes. Second Edition. W3C Recommendation, 28 October 2004.

[23] A. Zugenmaier, M. Kreutzer, and M. Kabatnik. Enhancing applications with approved location stamps. In *IEEE Intelligent Network 2001 Workshop (IN2001)*, 2001.