Spatial-Temporal Certification Framework and Extension of X.509 Attribute Certificate Framework and SAML Standard to Support Spatial-Temporal Certificates

Ana Isabel González-Tablas Ferreres, Benjamín Ramos Álvarez,
and Arturo Ribagorda Garnacho

Computer Science Department, Universidad Carlos III de Madrid (Spain)
{aigonzal,benja1,arturo}@inf.uc3m.es

Abstract. The recent development of location-based services has originated a set of new security services that address their particular security problems. Spatial-temporal certification services are among these new services. They have as main goal the generation of evidences about an entity's spatial-temporal information and, in general, their life-cycle support. Currently there is still a lack of a general framework for spatial-temporal certification services. In this work it is presented such a framework and an extension of the X.509 attribute certificate framework and the SAML standard to represent spatial-temporal certificates.

Keywords: Spatial-temporal certification, X.509 AC, SAML.

1 Introduction

Last decade has witnessed the development and commercial deployment of location-based services. As some authors have pointed out, security is a major challenge in location-aware computing [PMP03]. Trust (authenticity and attestation) and privacy of location information stand out as main security requirements. Several mechanisms have been proposed to address trust of location information, mainly location authentication protocols and spatial-temporal attestation services, which include spatial-temporal certification services. A brief survey on mechanisms that address trust of location information can be found in [GKRR05]. A survey on mechanisms to protect location privacy in pervasive computing can be found in [GTH05].

This work focuses on spatial-temporal certification services. Although several authors have proposed spatial-temporal certification models and mechanisms, there is still a lack of a general framework that defines their goals, model and requirements. This work presents a basic spatial-temporal certification framework and an extension of the X.509 attribute certificate framework [ITU05] and the SAML standard [OAS05] to represent spatial-temporal certificates.

Related work. During the last decade some spatial-temporal certification models and mechanisms have been proposed in [ZKK01, Bus04], but none of them addresses the definition of a general spatial-temporal framework, instead they focus on specific application scenarios. Zugenmaier, Kreutzer and Kabatnik propose a model and a mechanism to provide location stamps for subscribers of the GSM mobile network. Bussard defines a type of privacy-enhancing certificates which he proposes to use, among other applications, in location- and time-stamping. Furthermore, neither Zugenmaier *et al.* nor Bussard do specify the structure of the spatial-temporal certificates using any of the current attribute certificate standards. Within IETF GEOPRIV WG, a location object format has been defined for carrying location information on the Internet [IET05]; digital signatures have been proposed to protect the integrity of this location object but it is not meant to be a proper certificate. Besides, GEOPRIV, in collaboration with the Open GIS Consortium [OGC06], is currently working on the definition of an interoperable geodetic representation worth of taking into account.

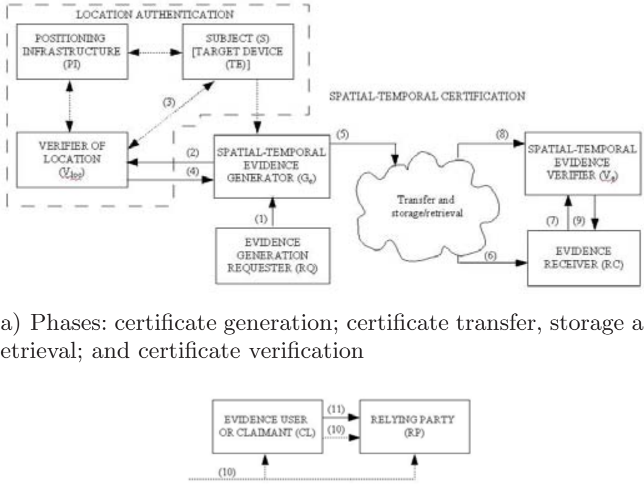
Paper outline. Section 2 presents the basic spatial-temporal certification framework and Section 3 the proposed extensions of the X.509 AC framework and the SAML standard. Section 4 presents the conclusions and future work that have been identified from this research.

2 Spatial-Temporal Certification Framework

2.1 Goal and General Model

Similar to the definition for non-repudiation services in [ISO97], spatial-temporal certification services are defined as *those services that generate, collect, maintain, make available and validate evidences concerning the spatial-temporal information of an entity.* Spatial-temporal certification services must be provided, as well, within the context of a security policy. Among their applications stand access control to services or resources based on the location of the requester entity. For example, an on-line gambling site may require that, in order to grant access to the site, their clients must be located within some specific geographic area, or a shopping centre may desire to grant privileges depending on users' visiting history. Another application is found in non-repudiation scenarios, e.g., to provide non-repudiation and accountability in the tracking of entities and assets, such as mobile workers, vehicles, ships, hazardous materials or valuable assets. In addition, spatial-temporal evidences can be used to provide non-repudiation and accountability in location-based billing, as in automatic toll collection systems, for highway usage or for entrance in certain areas (high populated urban areas or preserved environmental zones such as biosphere reserves).

Several entities performing a number of roles may be involved in the provision of spatial-temporal certification services (see Figure 1). First, the *evidence generation requester* (RQ) is who requests the generation of a spatial-temporal evidence. The *spatial-temporal evidence generator* (G_e), is in charge of generating the evidences, and probably also collects, maintains and makes them available. The *evidence receiver* (RC) is who obtains the spatial-temporal evidence after it


LOCATION AUTHENTICATION
POSITIONING INFRASTRUCTURE (PI)
SUBJECT (S) [TARGET DEVICE (TD)]
SPATIAL-TEMPORAL CERTIFICATION
VERIFIER OF LOCATION (V_loc)
(3)
(2)
(4)
SPATIAL-TEMPORAL EVIDENCE GENERATOR (G_e)
(5)
(1)
EVIDENCE GENERATION REQUESTER (RQ)
Transfer and storage/retrieval
(8)
SPATIAL-TEMPORAL EVIDENCE VERIFIER (V_e)
(7)
(9)
(6)
EVIDENCE RECEIVER (RC)
EVIDENCE USER OR CLAIMANT (CL)
(11)
(10)
RELYING PARTY (RP)
(10)

(a) Phases: certificate generation; certificate transfer, storage and retrieval; and certificate verification

(b) Phase: certificate use

Fig. 1. General model of spatial-temporal certification services (dispute resolution phase is not shown)

has been issued. Evidence receivers should be able of verifying the evidence; the *spatial-temporal evidence verifier* (V_e) performs this task.

The entity which the evidences refer to is the *subject* (S) of the evidence, that is, the spatial-temporal information asserted in the evidence refer to the subject. The subject must be, at least, a positionable device; in addition, the subject of the evidence may also refer to the user controlling the target device. Subjects should be uniquely identifiable according to some identification scheme. It is assumed that the spatial-temporal information of the subject is securely verified or authenticated before the evidence is generated. The *verifier of location* (V_{loc}) performs this verification in collaboration with a positioning infrastructure (PI); this process is done by executing a location authentication protocol (see a description and an analysis of this kind of protocols in [GKRR05]). Note that considering the user controlling the target device as part of the subject would require to verify also the proximity of this particular user to that target device. It is assumed that G_e trusts V_{loc} and PI to obtain authentic spatial-temporal information about the subjects under certain security model.

The use of the evidence must be done within the context of the policy under which the evidence has been issued. 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 payment). The *relying party* (RP) is the entity that provides some benefit to the claimant based on the evidence and maybe other auxiliar information. An entity may assume several of the presented roles. Some of them may be performed by trusted third parties (TTP) or trusted platform modules (TPM). Other TTPs may also be involved in the service provision.

Spatial-temporal certification services comprise mostly the same phases as non-repudiation services do [ISO97] (see Figure 1 for the numbers in brackets):

- *Certificate generation.* RQ asks G_e to generate a spatial-temporal certificate on certain subject S (step 1). G_e verifies the request and asks V_{loc} to locate subject S at that moment (step 2). V_{loc}, in collaboration with PI, verifies or authenticates the location of the subject (step 3) and returns to G_e this information (step 4). Finally, G_e generates the spatial-temporal certificate.
- *Certificate transfer, storage and retrieval.* G_e may store the evidence in a repository or transfer it to the receiver entity RC (steps 5 and 6). RC may also retrieve the certificate from the repository by himself afterwards.
- *Certificate verification.* In this phase, RC requests V_e to verify the evidence (step 7), who may need to retrieve the evidence or some additional information (step 8). The result of the verification is returned to RC (step 9).
- *Certificate use.* The evidence should have been transferred either to CL or to RP (step 10) and it is used by CL to obtain some benefit from RP (step 11). RP should verify the evidence before deciding to grant any benefit.
- *Dispute resolution.* If CL and RP do not agree regarding the benefit granting, both parties may leave the decision to an adjudicator, who will resolve the dispute taking into account the available evidences and the policies under which the evidences have been issued. This phase is not always needed.

2.2 Requirements

Establishment of trust on the evidence. Users of the evidence must be able to establish trust on the information certified in the evidence; therefore:

R1.1. Evidences must bind a subject to certain spatial-temporal information.
R1.2. It must be possible to verify who is the evidence author (data origin authentication) and that the evidence has not been modified (data integrity).
R1.3. It should be able to determine the source of the spatial-temporal information asserted in an evidence and the method used to obtain it.
R1.4. It must be possible to determine the temporal validity of an evidence.
R1.5. It should be able to determine the accuracy of the spatial-temporal information asserted in the evidence.
R1.6. It may be able to bind a particular subject with several spatial-temporal information tokens.

Spatial-temporal certification policy. As in non-repudiation services [ISO97], spatial-temporal certification services must be provided within the context of a particular spatial-temporal certification policy; therefore:

R2.1. It must be possible to determine the security policy under which a spatial-temporal evidence has been issued.

Protection of spatial-temporal information privacy. Location information is considered by many legislation corpus as personal data if it can be direct or indirectly associated to an identified or identifiable entity [Dir02]. It is usually required that affected users consent the processing of their personal data after having been informed of the characteristics of its processing. Spatial-temporal evidences can be considered personal data as spatial-temporal information is bound to some particular subject. These requirements have been identified:

R3.1. Users must be able to control the circumstances under which the spatial-temporal information of their target devices is processed.
R3.2. As a consequence of requirement R3.1, confidentiality of spatial-temporal information must be guaranteed according to user's preferences.
R3.3. It should be able to determine which user's privacy preferences concern a certain spatial-temporal evidence.
R3.4. Spatial-temporal certificates may support use of privacy-enhancing certificates (such as the ones proposed in [Bus04]).
R3.5. Users may be able to specify bounds on spatial-temporal resolution to be used in the spatial-temporal information included in evidences.

Supporting functionalities

R4.1. Support functionalities must be provided to generate, store, retrieve, verify, show and delete spatial-temporal evidences.
R4.2. Support may be provided to automatize some spatial-temporal processes such as evidence generation.
R4.3. Support may be provided to automatize the enforcement of users' privacy preferences.

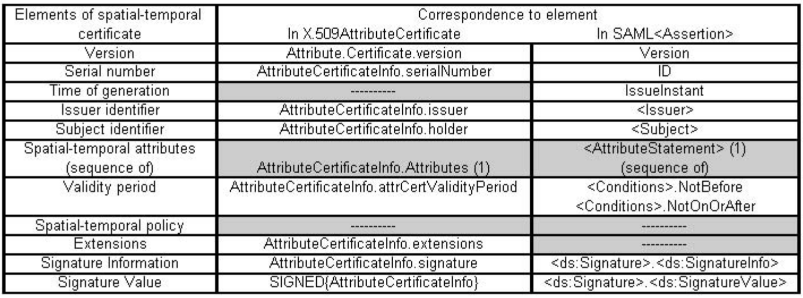
2.3 Mechanisms to Provide Spatial-Temporal Certification Services

Digital signatures are one of the most common mechanisms used to generate digital evidences. In particular they have been standardized as the mechanism to bind attributes to some entity in the ITU-T X.509 attribute certificate framework [ITU05] and the mechanism to protect the integrity and the issuer authentication of the assertions defined in the OASIS SAML standard [OAS05]. The verification of certificates based on digital signatures usually consists in verifying the signature's correctness and validity. Both X.509 attribute certificates (or its PKIX profile [IET02]) and SAML attribute assertions can be used as baseline to define spatial-temporal certificates.

To fulfill requirement blocks 1 and 2, a spatial-temporal certificate generated with a digital signature mechanism should contain the elements in the first column of Figure 2. Spatial-temporal attributes should allow the specification of certain spatial information and its resolution, certain temporal information and its resolution, the identifier of the spatial-temporal information provider and the method used to obtain the position and time asserted in the attribute. Instead of this classical certificate structure, some of the new privacy-enhancing certificate format recently proposed may be used (e.g., [Bus04]). Privacy-enhancing certificates address in an elegant way some of the requirements in block 3, but other simpler solutions may also be used. For example, privacy can be provided with access control mechanisms or encryption of spatial-temporal attributes; these mechanisms can be complemented with the binding of the user's privacy preferences to the certificates. To provide support to this and future issues, it is advisable that spatial-temporal certificates allow arbitrary extensions, signed and unsigned. Finally, requirement block 4 should be provided by a certificate management infrastructure as the ones proposed for the X.509 AC framework, its PKIX profile or for SAML assertions.

3 Extension of X.509 Attribute Certificate Framework and SAML Standard

In this Section, two basic spatial-temporal certificate structures are defined to address requirement blocks 1 and 2. The X.509 attribute certificate framework and the SAML standard are used as base. Most of the elements composing a (classic) spatial-temporal certificate (as defined in Section 2.3) can find an equivalent element in the X.509 attribute certificate and the SAML attribute assertion structures. Figure 2 presents these pairs of equivalent elements and points out which ones have no equivalent (the cells are shown with grey background). To obtain a complete spatial-temporal certificate structure, X.509 attribute certificate and SAML assertion have to be extended in order to provide a solution for the greyed elements. Both certificate structures defined in this work limit subject's location representation to geodetic information.

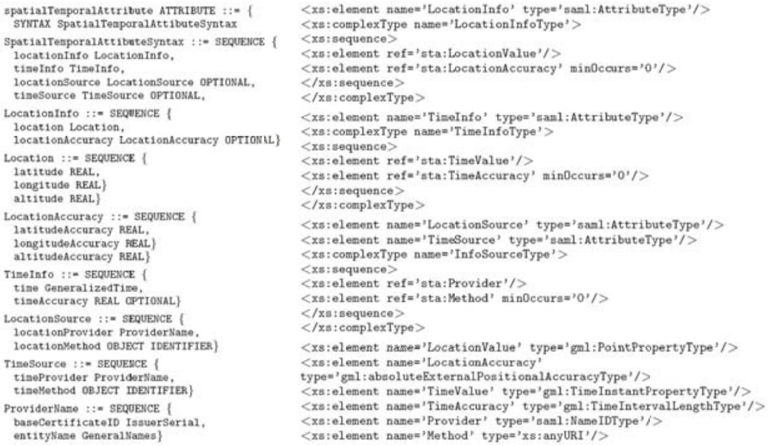


Elements of spatial-temporal certificate	Correspondence to element	
	In X.509AttributeCertificate	In SAML<Assertion>
Version	Attribute.Certificate.version	Version
Serial number	AttributeCertificateInfo.serialNumber	ID
Time of generation	----------	IssueInstant
Issuer identifier	AttributeCertificateInfo.issuer	<Issuer>
Subject identifier	AttributeCertificateInfo.holder	<Subject>
Spatial-temporal attributes (sequence of)	AttributeCertificateInfo.Attributes (1)	<AttributeStatement> (1) (sequence of)
Validity period	AttributeCertificateInfo.attrCertValidityPeriod	<Conditions>.NotBefore <Conditions>.NotOnOrAfter
Spatial-temporal policy	----------	----------
Extensions	AttributeCertificateInfo.extensions	----------
Signature Information	AttributeCertificateInfo.signature	<ds:Signature>.<ds:SignatureInfo>
Signature Value	SIGNED{AttributeCertificateInfo}	<ds:Signature>.<ds:SignatureValue>

Fig. 2. Correspondence between elements of spatial-temporal certificate and elements of X.509 attribute certificate and SAML attribute assertion. Greyed elements do not have equivalent element. Those marked with (1) have an equivalent element but it must be extended to fulfil spatial-temporal certificate requirements.

Basic X.509-based spatial-temporal certificate. In this case, the time of generation may be expressed as a `timeGeneration` extension element defined as `GeneralizedTime`. The `certificatePolicies` field defined in X.509 public-key certificate framework can be used in this case to specify the spatial-temporal certificate policy. X.509 attribute framework defines a general attribute certificate structure but application specific attributes must be defined as needed. A spatial-temporal attribute may be defined as shown in Figure 3(a). Note that a naïve spatial information element has been specified using a latitude-longitude-altitude tuple expressed in decimal degrees and meters but it should be desirable to use a generalized spatial representation (such a representation may be found in the ISO/TC 211 Geographic information/Geomatics standards).

Basic SAML-based spatial-temporal certificate. In this case, the spatial-temporal policy element may be defined as an XML attribute of a new SAML assertion (<`SpatialTemporalAssertion`>). Then, a new SAML attribute statement (<`SpatialTemporalStatement`>) is defined to contain the spatial-temporal attribute. Furthermore, four new SAML attributes are defined to express the location, the time, the spatial information source (provider and positioning method) and the temporal information source (see Figure 3(b)). Spatial and temporal elements have been defined using types from the GML 3.1.1 standard [OGC04]. Note that the elements belonging to the name space associated with the <`SpatialTemporalAssertion`> element are prefixed with '`sta:`'; types from GML are prefixed with '`gml:`' and types from SAML are prefixed with '`saml:`'. Future extensions of the SAML-based spatial-temporal certificate may be specified with new attribute statements (this approach may also be used in the X.509-based structure).



```
spatialTemporalAttribute ATTRIBUTE ::= {
  SYNTAX SpatialTemporalAttibuteSyntax
SpatialTemporalAttibuteSyntax ::= SEQUENCE {
  locationInfo LocationInfo,
  timeInfo TimeInfo,
  locationSource LocationSource OPTIONAL,
  timeSource TimeSource OPTIONAL,
LocationInfo ::= SEQUENCE {
  location Location,
  locationAccuracy LocationAccuracy OPTIONAL}
Location ::= SEQUENCE {
  latitude REAL,
  longitude REAL}
  altitude REAL}
LocationAccuracy ::= SEQUENCE {
  latitudeAccuracy REAL,
  longitudeAccuracy REAL}
  altitudeAccuracy REAL}
TimeInfo ::= SEQUENCE {
  time GeneralizedTime,
  timeAccuracy REAL OPTIONAL}
LocationSource ::= SEQUENCE {
  locationProvider ProviderName,
  locationMethod OBJECT IDENTIFIER}
TimeSource ::= SEQUENCE {
  timeProvider ProviderName,
  timeMethod OBJECT IDENTIFIER}
ProviderName ::= SEQUENCE {
  baseCertificateID IssuerSerial,
  entityName GeneralNames}
```

(a) X.509 AC extension

```
<xs:element name='LocationInfo' type='saml:AttributeType'/>
<xs:complexType name='LocationInfoType'>
<xs:sequence>
<xs:element ref='sta:LocationValue'/>
<xs:element ref='sta:LocationAccuracy' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
<xs:element name='TimeInfo' type='saml:AttributeType'/>
<xs:complexType name='TimeInfoType'>
<xs:sequence>
<xs:element ref='sta:TimeValue'/>
<xs:element ref='sta:TimeAccuracy' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
<xs:element name='LocationSource' type='saml:AttributeType'/>
<xs:element name='TimeSource' type='saml:AttributeType'/>
<xs:complexType name='InfoSourceType'>
<xs:sequence>
<xs:element ref='sta:Provider'/>
<xs:element ref='sta:Method' minOccurs='0'/>
</xs:sequence>
</xs:complexType>
<xs:element name='LocationValue' type='gml:PointPropertyType'/>
<xs:element name='LocationAccuracy'
type='gml:absoluteExternalPositionalAccuracyType'/>
<xs:element name='TimeValue' type='gml:TimeInstantPropertyType'/>
<xs:element name='TimeAccuracy' type='gml:TimeIntervalLengthType'/>
<xs:element name='Provider' type='saml:NameIDType'/>
<xs:element name='Method' type='xs:anyURI'/>
```

(b) SAML extension

Fig. 3. Main extension elements to support basic spatial-temporal certificates

4 Conclusions and Future Work

Frameworks are important instruments for the security research community. A framework for a security service usually defines its goals, its general provision models and the requirements it should fulfill. Security frameworks may also describe specific mechanisms that allow the service provision. Recent development of location-based services has originated a set of new security services that address specific security problems for this context. Spatial-temporal certification services stand among these new services. In the last decade several authors have proposed spatial-temporal certification models and mechanisms [ZKK01, Bus04], but none of them addresses the definition of a general spatial-temporal framework. This work addresses the definition of such a spatial-temporal certification framework. A brief discussion on the mechanisms that may be used to provide spatial-temporal certification services is also presented. Authors do not have addressed an exhaustive definition of the framework, instead an initial but grounded baseline is presented in order to be used as discussion starting point. Furthermore, two specific spatial-temporal certificate formats are also proposed, based respectively on the X.509 AC framework and the SAML standard.

Lots of open issues remain unaddressed. A more general format of spatial information, able of representing different geographic places and semantic locations and taking into account interoperatibility issues, is needed. Both structures have to be extended to address requirement block 3, including in the framework privacy-enhancing certificates. Besides, integration with location authentication protocols should be properly analyzed. Finally, implementations of spatial-temporal certification service demonstrators must be developed. We are currently working on such an implementation, which will issue, at first, SAML-based certificates; privacy requirements are being addressed with an access control system based on generalized role-based access control model [MA01].

Acknowledgment

The authors would like to thank the referees. Authors are supported by "Dirección General de Investigación del M.E.C." under contract SEG2004-02604.

References

[Bus04] Bussard, L.: Trust Establishment Protocols for Communicating Devices. PhD thesis, Institut Eurécom, Télécom Paris (2004)

[Dir02] 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)

[GKRR05] González-Tablas, A.I., Kursawe, K., Ramos, B., Ribagorda, A.: Survey on location authentication protocols and spatial-temporal attestation services. In: Proc. of IFIP Intl. Symposium on Network-Centric Ubiquitous Systems (2005)

[GTH05] Görlach, A., Terpstra, W.W., Heinemann, A.: Survey on location privacy in pervasive computing. In: Proc. of the Workshop on Privacy, Security and Trust within the Context of Pervasive Computing, Kluwer, Dordrecht (2005)

[IET02] IETF (Internet Engineering Task Force). An Internet Attribute Certificate Profile for Authorization (RFC 3281) (2002)

[IET05] IETF (Internet Engineering Task Force). A Presence-Based GEOPRIV Location Object Format (RFC 4119) (2005)

[ISO97] ISO/IEC. ISO/IEC 10181-4. Information technology - OSI - Security frameworks in open systems - Part 4: Non-repudiation framework (1997)

[ITU05] ITU-T. RECOMMENDATION X.509 - The Directory: Public-key and attribute certificate frameworks (2005)

[MA01] Moyer, M.J., Ahamad, M.: Generalized role-based access control. In: Proc. of Intl.Conf. on Distributed Computing Systems, IEEE Computer Society Press, Los Alamitos (2001)

[OAS05] OASIS. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) Version 2.0. OASIS Standard (2005)

[OGC04] OGC (Open Geospatial Consortium Inc.). OGC 03-105r1: OpenGIS Geography Markup Language (GML) Implementation Specification (February 2004)

[OGC06] OGC. OGC 06-142: GML 3.1.1 PIDF-LO Shape Application Schema for use by the Internet Engineering Task Force (IETF) (December 2006)

[PMP03] Patterson, C.A., Muntz, R.R., Pancake, C.M.: Challenges in location-aware computing. IEEE PervasiveComputing 2(2), 80–89 (2003)

[ZKK01] Zugenmaier, A., Kreutzer, M., Kabatnik, M.: Enhancing applications with approved location stamps. In: Proc. of IEEE Intelligent Network Wks. (2001)