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

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 321–329, 2007.

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