# Chapter 4
# Security and Licensing for Geospatial Web Services

**Bastian Schäffer**
*University of Münster, Germany*

**Rüdiger Gartmann**
*Conterra GmbH, Germany*

## ABSTRACT

*This paper presents an approach for enabling the commercial use of Geospatial Web Services in an on demand and ad-hoc fashion. The main goal is to go beyond classical Role-Based Access Control models in order to support ad-hoc license agreements directly in-process, without any prior offline negotiated agreements being necessary between georesource provider and geoprocessing user for on-demand access. Therefore, a general security and licensing architecture is defined as a transparent layer for Geospatial Web Services. In particular, this chapter focuses on state-of-the-art interface specifications from OGC and defines generic security extensions being applicable to all OGC standards based on OWS Common. The static model with trust relationships between the different components of the architecture in heterogeneous security domains as well the dynamic structure is studied. The presented ideas are verified by a proof-of-concept implementation following a real world scenario.*

## 1 INTRODUCTION

Geospatial Web Services organized in a Spatial Data Infrastructures (SDIs) are designed for the purpose of providing and sharing georesources (data and models) across organizational and technical boundaries. The real potential lies in the agility of Geospatial Web Service via SDIs to access external georesources on-demand and to integrate them into business process on the fly (Groot & McLaughlin, 2000). This goal is mostly reached on a technical level by the provision of data encoding and service interface standards, such as established by the Open Geospatial Consortium (OGC).

DOI: 10.4018/978-1-60960-192-8.ch004

However, partners will only conduct business if their (geo)rights, trust and security requirements are met. Therefore, a general security architecture has to be defined as a transparent layer for Geospatial Web Services. In particular, this chapter will focus on state-of-the-art interface specifications from OGC and will define generic security extensions being applicable to all OGC standards based on OWS Common (OGC, 2006b). On an abstract level, such extensions should be independent of specific technology bindings, leading to a common abstract security architecture for OGC Web Services.

But besides the technical challenge, there is a legal barrier still in place, obstructing especially the commercial use of Geospatial Web Services. For commercial use, it is necessary to establish an agreement between georesource provider and georesource user regarding the terms and conditions of use regarding the specific georesource (OGC, 2006a). It is easily imaginable that this time-consuming way of licensing clearly contradicts the goal of seamless integration and agile interaction. This gap was also identified by INSPIRE (Infrastructure for Spatial Information in Europe), resulting in the demand for e-commerce services in the INSPIRE Directive, Article 14(4) (EU, 2007). Therefore we aim at going beyond classical Role-Based Access Control (see section 2.5) models in order to support ad-hoc license agreements directly in-process, without any prior offline negotiated agreements being necessary between georesource provider and geoprocessing user for on-demand access. This will give us the flexibility to support on-demand scenarios and fully support the SDI publish-find-bind pattern on an ad-hoc basis with prior unknown and untrusted entities.

This paper gives first a thorough overview of general security concepts such as authentication, authorization, cryptography and trust in a Geospatial Web Services context. This is followed by a two folded concept. At first, general security and licensing requirements for Geospatial Web Services are analyzed. This is followed by a specific security architecture, which includes a description of how standard SDIs can be enhanced in order to support ad-hoc license agreements directly in-process, without any a priory settled rights or trust relationships being necessary between data provider and data user. This also includes the aspects of license encodings, security to enforce license-conformant access to services, metadata extensions to inform about license- and security-related requirements of a certain service, protocol extensions to submit license and identity information between the communicating parties and federation concepts in order to establish trust between initially unknown parties.

Finally, these ideas are verified by a real world scenario, which serves as a proof-of-concept realization.

## 2 BACKGROUND

This section provides a review of basic concepts and related work in the context of rights management, security and licensing for Geospatial Web Services.

### 2.1 Web Service Security

The definition of computer security in general has been defined in multiple ways, as i.e. by (Gollmann, 1999) (Bishop, 2005). For this chapter we rely on ISO as an international accepted standardization body, which defines it as:

"Information held by IT products or systems is a critical resource that enables organisations to succeed in their mission. Additionally, individuals have a reasonable expectation that their personal information contained in IT products or systems remain private, be available to them as needed, and not be subject to unauthorised modification. IT products or systems should perform their functions while exercising proper control of the information to ensure it is protected against hazards