DESIGN SECURITY AND GEO-RIGHTS MANAGEMENT SERVICES IN SPATIAL DATA INFRASTRUCTURE

Tomasz Kubik[1], Witold Paluszyński[1], Bartosz Kopańczyk[2], Adam Iwaniak[3], Paweł Netzel[4]
1 Institute of Computer Engineering, Control and Robotics, Wroclaw University of Technology, Janiszewskiego 11/17, Wroclaw, Poland
2 GeoScope, Inc., Wrocław, Poland,
3 Institute of Geodesy and Geoinformatics,Wroclaw University of Environmental and Life Sciences, Norwida 25/27, Wroclaw 50-375, Poland
4Institute of Geography and Regional Development, University of Wrocław, Poland,
e-mail: {tomasz.kubik|witold.paluszynski}@pwr.wroc.pl,
bartek.kopanczyk@gmail.com, iwaniak@ar.wroc.pl, netzel@meteo.uni.wroc.pl

Abstract

Service-oriented architecture (SOA) is a concept of services, architecture and infrastructure that is being widely adopted in a geospatial information domain. It provides foundation for searching, obtaining and viewing spatial information in a distributed environment. The key actors on the scene are service providers and service consumers interacting remotely trough the Internet via HTTP protocol. However, because of open nature and features (such as service bus, service composition, and service virtualization) SOA adoption requires radical changes in the way the information resources are being developed and managed. The needs of setting up a new set of security requirements becomes substantial.

Numerous studies on the security subject have been conducted in the IT domain. They resulted with security standards propositions which vary in degree of completion and commercialization, and even occasionally compete. The deficiencies in the open standards definitions are sometimes covered by the proprietary solutions implemented by the security software vendors, but they are related to the vendor technology and distributed on a commercial bases. Regarding geospatial information the research on securing data and services has not been finalized yet. Most recent spatial data infrastructure implementations follows the SOA paradigm and open standards defined by the OGC, ISO and INSPIRE. These standards include specification of GeoDRM architecture (digital rights management) and GeoREL (rights expression language, ISO/CD 19149) for geographic information.

The article touches the problem of securing geospatial data and web services focusing on architecture of authorization services based on open standards and technologies. A special attention was given to the access protection to the OGC Web Mapping Services layers and other OGC Web Services. As a result some architecture scenarios were introduced and discussed together with the uniform supervised access mechanism to the functionality of the system components. Some security issues and solutions were

discussed that have come about as a result of web services and their related technologies use and are compliant to the GeoRM requirements.

1. Introduction

The creation of GIS production systems requires appropriate mechanisms, that restrict selected functionality and data from unauthorized use (Bishr, et al., 2007, FGDC, et al., 2006). Systems operating in a distributed manner are composed of a number of components, often located in different places of the network and using various technologies (Tait, 2005). There are many methods to ensure the safety of each of these components-services. However, adequate regulations are lacking at the national and European level, which would outline the appropriate methods for managing permissions and access rights to specific functionalities.

This problem concerns not only the geospatial services, but all of a wide range of industry groups that use their services for distributed solutions. According to the research conducted by CA in which 555 IT companies around the world took part, almost half of them (43 percent) considered security risks as a key issue in the implementation of software, based on the concept of SOA (Service Oriented Architecture). The integration of the security systems of distributed services into the existing solutions for identity and access rights management is therefore critical to their deployment. Jamkhedkar, et al. (2009) described issues related to the DRM architectures. Some snares that must avoided to end up with SOA security that makes sense were discussed by MacGraw. More information on securing SOA are provided by ORACLE (2008) and Dubnin (2008).

The dissemination of growing amounts of data does not go hand in hand with developing good practices in the management of the rights to use them. This results in the emergence of serious challenges in maintaining the confidentiality of data. To a certain extent these issues are addressed by metadata, which contain information on the restrictions on the use of data. Unfortunately, there is no close relationship of these restrictions with the mechanism of the authorization of users.

2. Security in access to service and data in IT systems

A major difficulty in building interoperability between systems using the WebServices technology is to ensure an adequate standard of communication in order to achieve a secure exchange of access rights. Under ideal conditions this is a new service, that would supervise the exchange of information between the services in a way that is transparent and independent of the participating components (Kiehle, 2006).

Authentication can be divided into two layers: one layer for controlling access to the functionality of the system, and second layer that controls access to the functionality of the network services. It would be best to merge these two layers and have one consistent feature, by transferring authority from the system level to the level of the internal components.

The safest solutions use the two- or multicomponent identification, while the weakest - but most widely used traditional mechanisms - are based on user names and passwords. There are intermediate solutions, based on encryption keys, certificates, and different types of software or hardware mechanisms. There is no standard identity management system. Authentication services, for example, often are done at the operating system level.

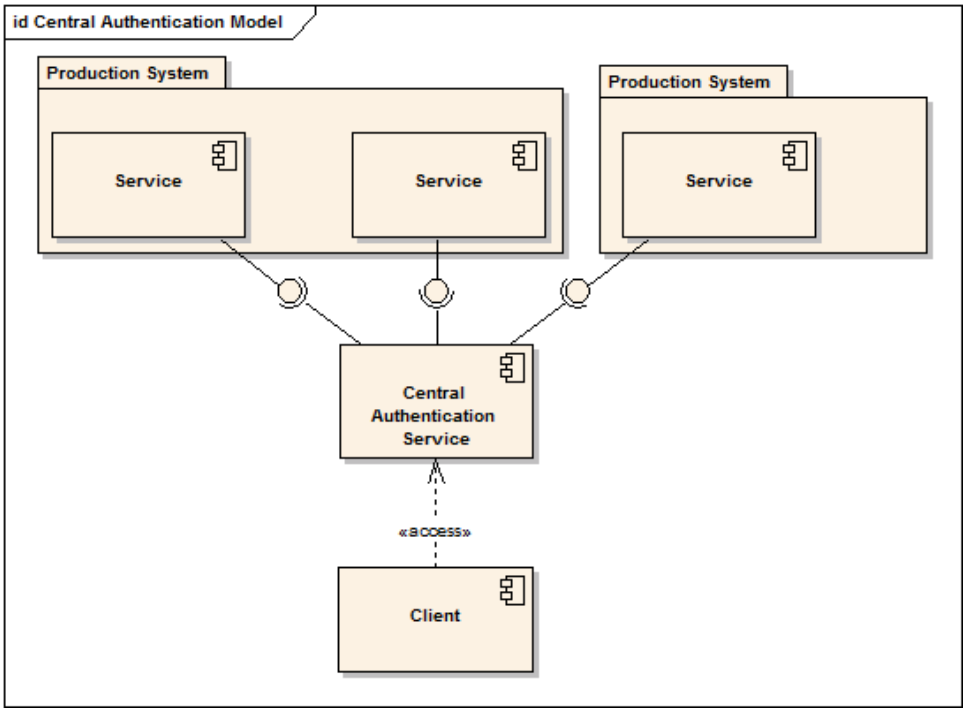

Figure 1: Central Authentication Model – concept architecture.

Some companies attempt to introduce rights management solutions as a centralized and closed systems. They work only for selected products of the same manufacturer and may be used in the broader scope by providing a suitable interface through which other components can communicate. One such solution is the Oracle Application Server Identity Management. This technology provides a way for communication between distributed services, where password and user data are located in a database dedicated for this purpose. It also supports the administration of rights through the introduction of a service called Delegated Administration Service (DAS), which gives the implementing entities access to a powerful and flexible solution. However, this is a proprietary solution which is too complicated to adapt in a technologically diversified system.

In the years 2001-2009 there appeared initiatives of the groups trying to unify the identity management schemes. One of these is the Liberty Alliance Project (LAP), which aims to establish a range of solutions based on open standards. The protocol has been developed, called OpenID - a system of identification and confirmation of identity, which allows for single sign-on (SSO) to different services. Personal data are given

once - to the operator of the identification system, which will then automatically make them available to other services. This technology came as a response to the LiveID solution (formerly known as. NET Passport) from Microsoft, which used Microsoft's proprietary .NET framework. LAP participated in the drafting of the SAML specification (Security Assertion Markup Language), subsequently taken over by OASIS. SAML is a mechanism of the exchange of information between services that authorize a process. Figure 1 represents communication between client and distributed production systems (based on SOA) thorough single sign-on mechanism.

3. Security in access to services and data in GIS geoportals

Article 14 of the Directive specifies the possibilities of payment regulations for access to spatial services provided by public authorities. It further mentions on the use of services in the field of electronic commerce, licensing, and other mechanisms to ensure the preservation of rights and security of transactions. In INSPIRE network services architecture such tasks are to be implemented using GeoRM services.
In general the GeoRM services should facilitate using a variety of mechanisms governing access to INSPIRE bus services. Examples of features offered by GeoRM services may be: authorization, authentication, pricing, billing, licensing access to the data (limited in time, spatial extent, specific position, particular user, etc.) (Vowles, 2006, FGDC, 2006, Bishr, 2007).

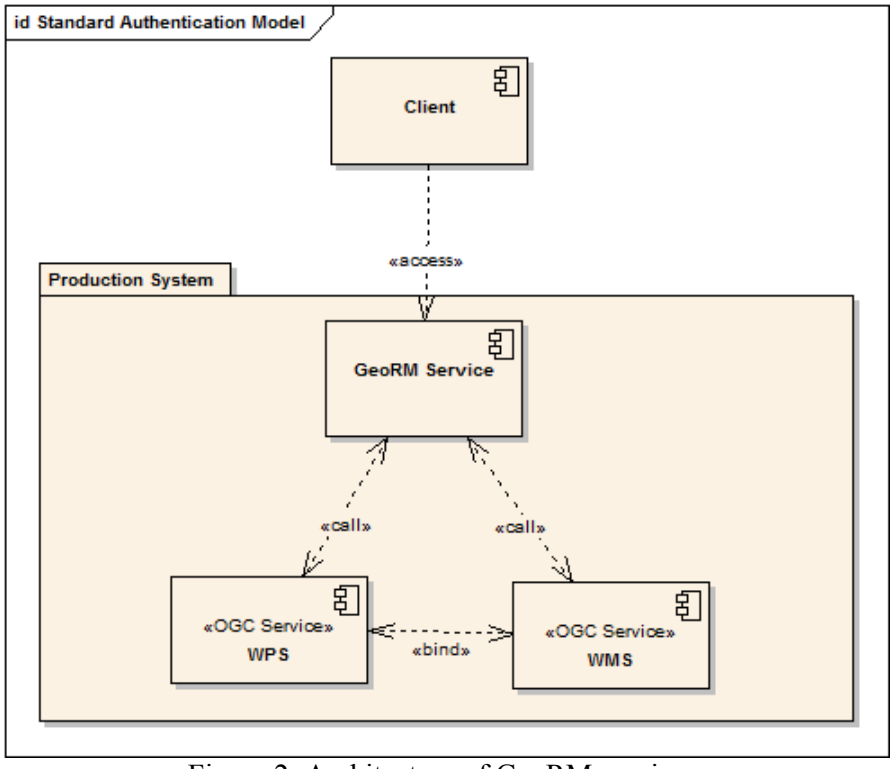

Figure 2: Architecture of GeoRM services.

Since verifying the capabilities or negotiating a contract for a service usually takes place between locating a service (finding) and using it (linking), the basic model has been extended for the INSPIRE architecture with the GeoRM layer from the standard "publish-find-bind" to the "publish-find-link-bind" form. The reconciliation phase occurs when access to the resources actually is governed by some law. If the user does not possess these rights, the application invoked by her should return to the previous state by raising an exception.

The process of passing the user's request to the selected service through the GeoRM layer, and returning the results, can be compared to filtration. The request, containing beside the basic parameters additional data such as: license keys, tokens, user name, etc., encounters in the GeoRM layer a series of GeoRM services. Passing through this layer it clears subsequent services - GeoRM filters - ending up in the target service. At the end the request contains only the parameters needed to invoke the service. After successful completion of the call its result returns to the user, again passing through the GeoRM layer. Under such scheme using a "blank" filter would be equivalent to directly calling a service.

Figure 2 shows the general service communication in GeoRM model. Client connects with every service in production system thorough transparent to them GeoRM service.

The implementation of GeoRM services may require certain data sets to be kept, such as user address, user ID, a license key, etc. Moreover, in order to meet the necessary requirements posed by the GeoRM layer it may be necessary to create user accounts globally for the infrastructure.

At this stage of the implementation of the INSPIRE directive the GeoRM layer is not required. Hence the need for harmonization of GeoRM data models will appear only when such data are used throughout the INSPIRE infrastructure. (This fact does not contradict using the existing mechanisms for security and geo-applications - the directive aims to combine infrastructures in a coherent system). The development of the GeoRM model services is carried out by OGC.

4. Examples of architectures

The architecture of authorization services introduces a uniform mechanism to supervise access to the functionality of the subsystem concerned. In practice, it is not possible to define one OGC service, which would supervise transparent authentication functionality to each subsystem. Therefore, each of the internal OGC services has a dedicated authorization service. A client connects to a central system service and after a successful authentication gets the key to the functionality of internal services. During the communication between the client and the internal services, the key is passed in the query to the service verifying the access rights. A filter is created dynamically that modifies the request and removes part of the result incompatible with the privileges. The whole process is supervised by the central authorization service, which makes it possible to manage privileges levels and groups of users.

For increased security the key is encrypted with an appropriate mechanism, which is understood by all services. Most encryption uses a public key or a certificates (like: CA

- certification authority, PKI - public key infrastructure). Less frequently, asymmetric encryption is used (simple key). When the security of the key and the data returned is important to the functionality of the system, in addition, they are transmitted through an encrypted connection (commonly: SSL - Secure Socket Layer).

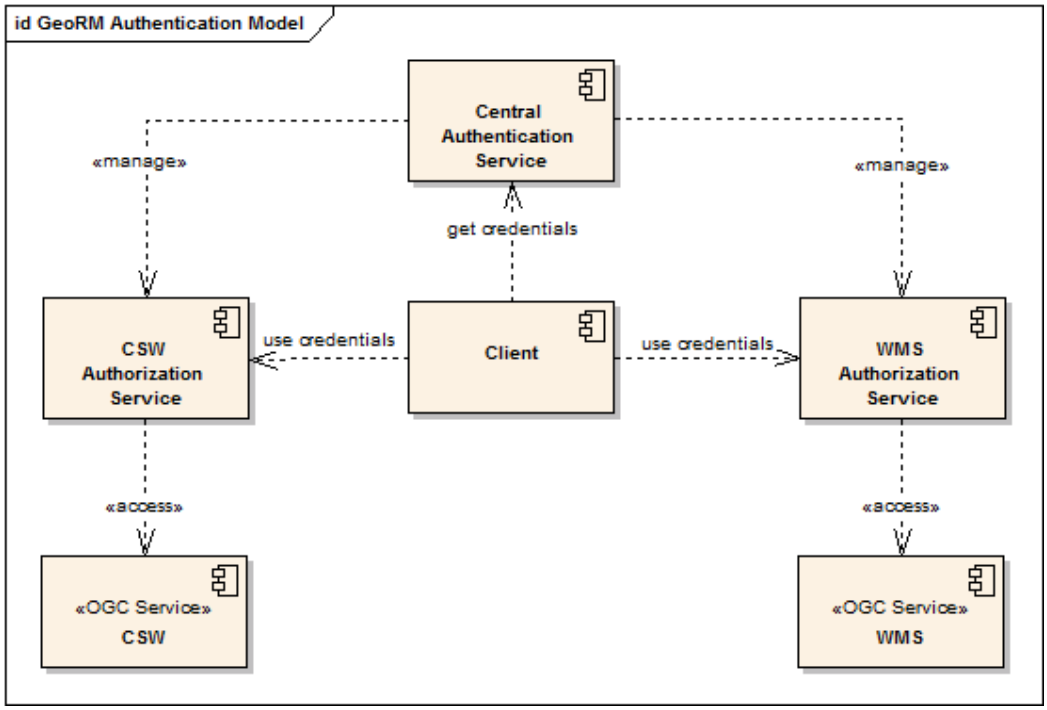

Figure 3: Interaction between internal services in GeoRM model.

An example implementation of this architecture are the components of German North52 project devoted to the development of WAS (Web Authorization Service). This service can be used as a homogeneous component, which manages the rights to the system in accordance to the OGC architecture and the GeoRM guidelines. The SAML credentials technology used in its implementation combines user authentication (Java Authentication and Authorization Service - JAAS) with the configuration method of another service - the WSS (Web Security Service), which supervises the client access to the specific WMS layers. The process of delegation of authorities is done with SAML credentials.

Since a significant part of the implementation of OGC services uses Java, the above technology can easily be integrated with application servers like Apache Tomcat, JBoss, or GlassFish. A rival solution to the JAAS technology is Spring Security (formerly known as Acegi Security for Spring). This technology has been used as part of the service securing access to the GeoNetworks open-source project, and may be used for establishing access control to the various layers of GeoServer WMS.

Figure 3 shows the interaction between a central authorization service (which can be performed by the previously mentioned North52 WAS), and example GeoRM services

authorizing access to OGC components. (For the WMS service the WSS service or Spring Security technology can be used). It should be noted that none of the OGC services has to be modified, since the management of access rights to their functionality is done at a higher layer.

5. Implementation of the elements of the Polish local SDI based on GeoRM model

The authors are working on a project whose goal is to promote the use of free software to implement SDIs at a local level (Iwaniak & Sliwinski , 2007, Kubik, et al. 2008). According to the official strategy in Poland, NSDI is implemented by the infrastructure nodes, which are at the local surveying and mapping agencies. The data they provide to their customers, eg. the geodetic points, can conveniently be implemented as a web service. Such service must be compatible with existing state laws and rules for data sharing in Poland.

During the preparation of a draft system to share the geodetic points, the authors analyzed the requirements for the system, as well as the available FOSS software. A configuration of PostgreSQL, Geoserver, OpenLayers + Dojo was selected as easy in administration and maintenance. It was important that the configuration of FOSS software did not constrain the operating system choice (Windows, Linux, or MacOS) to suit any user requirements. Figure 4 represents technologies used to create components of the system.

In terms of controlling access to data a built-in protection system ACEGI was used. It allows to control access to data and services provided by Geoserver according to the roles assigned to users. The usage of the ACEGI system enables the separation of access rights to data and the highlighting the layers of thematic maps provided both to anonymous and registered users.

An anonymous user has only access to WMS services with the exception of GetFeature functionality. She only has access to a map without any possibility to download data objects (geodetic points). A registered user has access to the WFS service and can make selections and browse and download information describing the details of geodetic points. Downloading topographic names also requires authorization to the WFS service.

Since a standard configuration of Geoserver uses the HTTP Basic Authentication, the component responsible for authorizing users was replaced with JAAS. The user groups and their passwords are stored in dedicated XML files managed by JAAS. The module also controls access to all the components of the portal, using mechanisms built into Tomcat. For safety the passwords are hashed with MD5 (Message-Digest algorithm 5). The functionalities of JAAS and ACEGI have been merged and use the same XML files with user groups and passwords. The user data are passed by the JAAS authorization component to the system. In the case of using the WMS system, the ACEGI component acquires the user data and then, using the same configuration files, executes the filtration process on the query.

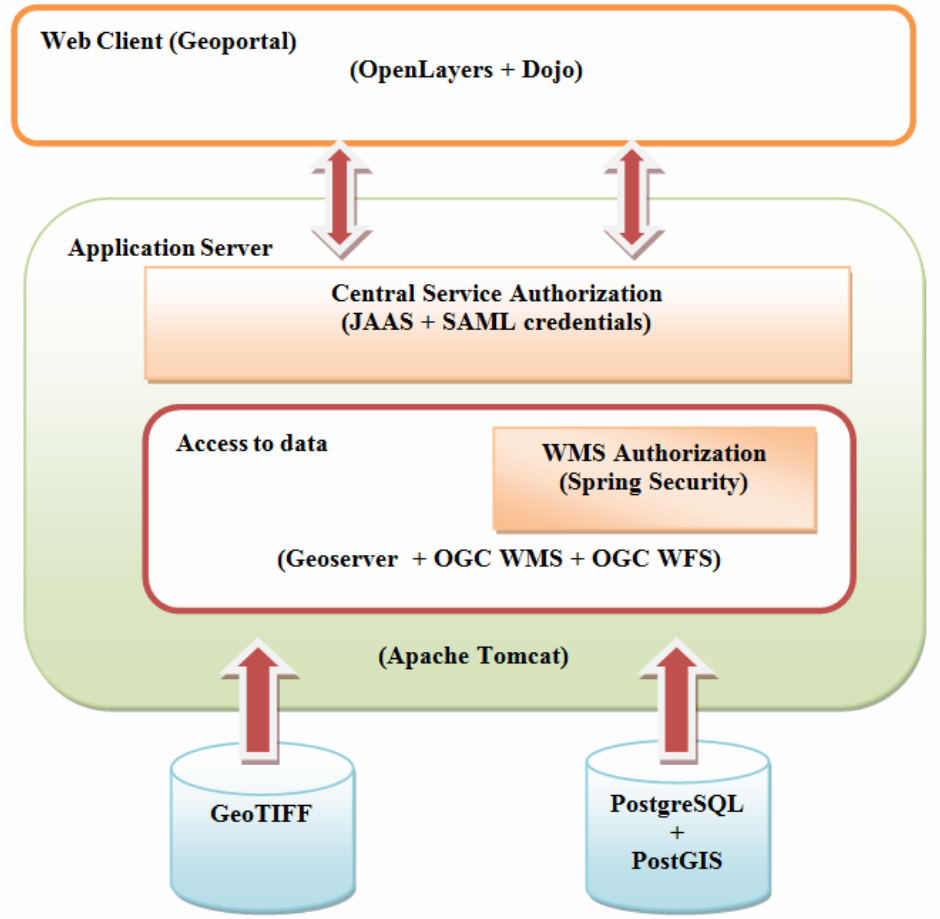

Figure 4: Architecture of the system to share geodetic points.

6. Summary

The article presents the variety of configurations for service oriented architecture. In order to ensure interoperability between the OGC services, it is proposed to use components that fit the GeoRM model proposed by the INSPIRE Directive. This architecture enhances the security of distributed GIS systems and automates the process of passing information related to the access rights for certain functionalities of services. In conjunction with the information provided by the cataloge services (OGC Catalog Services for Web - CSW) it is capable of effectively managing restrictions on spatial data or services. The metadata section that describes limitations of the spatial data or service should include detailed information permitting the client to learn in an automated way how it may demonstrate its right to use data and functionality from the service.

There exist many libraries, both commercial and free, which can be used to implement security mechanisms. It is important that these libraries be built into a service or services, which do not interfere with the existing model of the system, but extend it by creating a new layer of architecture conforming to the GeoRM requirements. With such a solution, the model will maintain interoperability not only with the internal components of the extended system, but can be used to establish communication between external systems.

Acknowledgements

This research was supported in part by the Ministry of Science and Higher Education through grant Nr R09 011 03.

References

Iwaniak, A. & Sliwinski, A., 2007, Using free software for SDI implementation (in Polish), Roczniki Geomatyki.

Kiehle, C., 2006, Business logic for geoprocessing of distributed geodata. Computers and Geosciences, 32(10):1746-1757.

Kubik, T. Paluszynski, W. & Netzel, P., 2008. Implementation of the Elements of the Polish National Spatial Data Infrastructure Based on Open Source Software,

ORACLE, 2008, Web Services Security: What's Required To Secure A Service-Oriented Architecture. Available at: http://www.oracle.com/technology/products/webservices_manager/pdf/Oracle-SOA-security-whitepaper-Jan08.pdf

Vowles, G., 2006, Geospatial Digital Rights Management Reference Model, OGC INC., OGC 06-004r3.

Tait, M.G., 2005, Implementing geoportals: applications of distributed GIS. Computers, Environment and Urban Systems, 29(1), pp. 33-47.

Bishr, M. Wytzisk, A. & Morales, J., 2007. Concepts GeoDRM: Towards Digital Management of Intellectual Property Rights for Spatial Data Infrastructures. In: H. Onsrud, ed. 2007. Research and Theory in Advancing Spatial Data Infrastructure. ESRI Press, pp. 245-260

FGDC, GeoData Alliance & OGC, 2006. GeoDRM Final Report. Available at: http://geodataalliance.org/uploads/GeoDRM_Final_Report.pdf

Jamkhedkar, P. A. & Heileman, G. L., 2009. Digital rights management architectures. Computers and Electrical Engineering, Elsevier Science, 35(2), pp. 376-394

McGraw, G., Software Security and SOA: Danger, Will Robinson! IEEE Security & Privacy, Available at: http://www.cigital.com/papers/download/bsi12-soa.doc.pdf

Dubin, J., 2008. How to secure SOA. Available at: http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185_gci1320470,00.html#

Iwaniak, A. Kopańczyk, B. Kubik, T. Netzel, P. Paluszyński W., Przykłady budowy infrastruktury danych przestrzennych na poziomie powiatowym z wykorzystaniem wolnego oprogramowania., Roczniki Geomatyki. 2008, t. 6, z. 7, s. 7-14.