ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30280—2013

信息安全技术　鉴别与授权　地理空间可扩展访问控制置标语言

Information security technology—Authentication and authorization—Geospatial eXtensible Access Control Markup Language（GeoXACML）

2013-12-31 发布　　2014-07-15 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国科学院软件研究所、北京数字认证股份有限公司、北京信息科学技术研究院。

本标准主要起草人:冯登国、付艳艳、陈驰、张敏、洪澄、李昊、田雪、詹榜华。

引　言

近年来，随着地理信息服务的广泛应用，地理信息交互的安全需求也日益强烈。但在互联网应用场景中，缺乏关于地理信息属性和授权信息定义、访问控制实现的规范，地理信息和资源缺乏必要的保护。

本标准参考开放地理信息联盟（OGC）的文件 Geospatial eXtensible Access Control Markup Language（GeoXACML） Version 1.0，通过定义一种可用于表达访问权限的基于规则的策略语言，使得实现一个能够互操作的地理空间访问控制系统成为可能。

本标准是可扩展访问控制置标语言（XACML）的一种扩展。

信息安全技术　鉴别与授权
地理空间可扩展访问控制置标语言

1　范围

本标准规定了地理空间可扩展访问控制置标语言(GeoXACML)的几何模型、数据类型、几何体拓扑关系函数以及几何函数。

本标准适用于地理信息服务场景中访问权限的定义和实施。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069—2010　信息安全技术　术语

OGC 06-103r4 v1.2.0　地理信息实施准则　简单要素访问　第1部分:通用架构(OpenGIS® Implementation Specification for Geographic information-Simple feature access—Part 1:Common architecture)

OASIS. Conformance Tests for XACML 1.0 and 1.1[EB/OL]. [2004-03-25]. http://www.oasis-open.org/committees/download.php/6076/ConformanceTests.zip

3　术语和定义

下列术语和定义适用于本文件。

3.1

访问　access

对资源执行的一种操作。

3.2

访问控制　access control

一种保证数据处理系统的资源只能由被授权主体按授权方式进行访问的手段。

[GB/T 25069—2010,定义 2.2.1.42]

3.3

动作　action

对资源的操作。

3.4

适用策略　applicable policy

控制特定决策请求的策略和策略集。

3.5

属性　attribute

主体、资源、动作和环境的特征,该特征可以在谓词和目标中被引用。

3.6

授权决策　authorization decision

对请求是否授权的决策。包含以下组成部分：适用策略的评估结果，由 PDP 返回给 PEP；评估函数，输出结果为“同意”“驳回”或“不适用”；一个义务的集合（可选）。

3.7

包　bag

值的无序集合，可能包含重复的值。

3.8

条件　condition

谓词表达式，其评估结果可以是“True”“False”或“Indeterminate”。

3.9

合取序列　conjunctive sequence

使用逻辑与（AND）连接的谓词序列。

3.10

上下文　context

决策请求和授权决策的规范表述。

3.11

上下文处理器　context handler

一个系统实体，它把决策请求从原始请求格式转换成 XACML 规范形式，并把授权决策从 XACML 规范形式转换成原始应答格式。

3.12

决策　decision

规则、策略或策略集的评估结果。

3.13

决策请求　decision request

由策略执行点（PEP）发送给策略决策点（PDP）的消息，要求生成授权决策的请求。

3.14

析取序列　disjunctive sequence

使用逻辑或（OR）操作符连接的谓词序列。

3.15

效果　effect

规则的预期评估结果，只能为“同意”或“驳回”。

3.16

环境　environment

一组与授权决策相关的属性集合，独立于特定的主体、资源或动作。

3.17

命名属性　named attribute

属性的一个特定实例，具体值取决于属性名、类型、持有者和属性颁发者。

3.18

义务　obligation

策略或者策略集中定义的特定操作，PEP 在执行授权决策时，应执行该操作。

3.19

策略　policy

由管理层正式表达的总体意图和指向。

[GB/T 25069-2010,定义 2.3.27]

3.20

策略管理点　policy administration point

创建策略或策略集的系统实体。

3.21

策略组合算法　policy-combining algorithm

从多个策略中得到决策和义务的过程。

3.22

策略决策点　policy decision point

系统实体,负责评估适用策略并产生授权决策。

3.23

策略执行点　policy enforcement point

系统实体,它通过产生决策请求并执行授权决策结果进行访问控制。

3.24

策略信息点　policy information point

系统实体,是属性值的来源。

3.25

策略集　policy set

若干策略或其他策略集,策略组合算法和若干义务(可选)的集合,可以是其他策略集的组成部分。

3.26

谓词　predicate

关于属性的声明,可以评估其是否为真。

3.27

资源　resource

数据、服务或系统组件。

3.28

规则　rule

包含目标(target)、效果(effect)和条件(condition),是策略的组成部分。

3.29

规则组合算法　rule-combining algorithm

从多个规则得到组合决策的过程。

3.30

主体　subject

断言可能引用的属性的所有者。

3.31

目标　target

通过主体、资源和动作进行限定的决策请求集合,是规则(Rule)、策略(Policy)和策略集(PolicySet)评价的对象。

4 缩略语

下列缩略语适用于本文件。

1D：一维(One-Dimensional)

2D：二维（Two-Dimensional）

3D：三维（Three-Dimensional）

GeoXACML：地理空间可扩展访问控制置标语言（Geospatial eXtensible Access Control Markup Language）

GeoDRM：地理空间数字权限管理（Geospatial Digital Rights Management）

GeoDRM-RM：地理空间数字权限管理-参考模型（Geospatial Digital Rights Management-Reference Model）

GML：地理置标语言（Geography Markup Language）

ISO：国际标准化组织（International Organization for Standardization）

OASIS：结构化信息标准促进组织（Organization for the Advancement of Structured Information Standards）

OGC：开放地理信息联盟（Open Geospatial Consortium）

OWS：OpenGIS 网络服务

PAP：策略管理点（Policy Administration Point）

PDP：策略决策点（Policy Decision Point）

PEP：策略执行点（Policy Enforcement Point）

PIP：策略信息点（Policy Information Point）

SAML：安全断言置标语言（Security Assertion Markup Language）

SFS：SQL 简单要素实施准则(Simple Features Implementations Specification for SQL)

UML：统一建模语言（Unified Modeling Language）

URN：统一资源名称(Uniform Resource Name)

XACML：可扩展访问控制置标语言（eXtensible Access Control Markup Language）

XML：可扩展置标语言（eXtensible Markup Language）

5 GeoXACML 几何模型

本章定义了 GeoXACML 核心几何模型，它独立于本标准策略声明中几何体的编码。那些几何体实际上可以以不同的 XML 编码实现。本标准提供了多个扩展部分，每个扩展部分都定义了一套特定的编码。

任何满足 GeoXACML 的实现应支持至少一种几何编码方案(见附录 A、附录 B)，并能够支持下面列出的这些几何类型。

本标准使用的几何体编码方案所依赖的所有底层几何模型均可参见 OGC 06-103r4 v1.2.0。

为了应用一种灵活、直接的方案，使得几何数据类型同基本 XACML 说明相一致，本标准在 XACML 的基础上扩展了一种新的数据类型，其名为“urn：ogc：def：dataType：geoxacml：1.0：geometry”。即：任何一个几何体属性值、一个几何值构成的包或一个指向几何数据的指针，其在本标准策略中的数据类型总是“urn：ogc：def：dataType：geoxacml：1.0：geometry”。

对于数据类型为“urn：ogc：def：dataType：geoxacml：1.0：Geometry”的几何体，其属性值〈AttributeValue〉应可以表示成下列基本类型之一：

——Point（点）：一个 0 维的几何对象，在坐标空间中代表一个单独的位置。一个点有一个 x 坐标值，一个 y 坐标值。如果涉及到其他空间参照系统，它也可能有 z 和 m 的坐标值。

——LineString（折线）：多点之间线性插值生成的一段弧。每一个连续的点对定义一条线段。

——Polygon（多边形）：由一个外部边界和 0 个或多个内部边界定义的平面表面。

——MultiPoint（多点）：多个 0 维的几何集。多点的元素只限于点。

——MultiLineString（多折线）：多段弧，其中的元素是线。

——MultiPolygon（多边形）：元素是多边形的多个平面。

上述几何体应作为一个〈AttributeValue〉元素的子节点。不论封闭几何体的类型是什么，〈AttributeValue〉元素的“数据类型”属性应设置为“urn:ogc:def:dataType:geoxacml:1.0:geometry”。封闭几何体的编码应遵守对应编码扩展说明的语法规则。几何体可以为空。一个空几何体的编码也应与相关扩展的定义保持一致。一个空的几何体也可以用数据类型“urn:ogc:def:dataType:geoxacml:1.0:geometry”的一个空的〈AttributeValue〉来表示。

〈AttributeValue DataType=“urn:ogc:def:dataType:geoxacml:1.0:geometry”/〉。

在 GeoXACML 中的几何数据类型和 XML 在扩展中编码的数据类型有所不同。像在 SFS 的几何模型中，本标准中的几何数据类型是一个抽象的超类。这个超类的具体实例就是在扩展中定义的 XML 编码数据类型。

6 GeoXACML 空间函数定义

6.1 概述

本章定义本标准所使用的关系操作符和几何操作符。相关定义参见 OGC 06-103r4 v1.2.0。

因为本标准定义的函数返回值为一个几何体的包。因此，在实现中应该提供数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的包。如果在策略中显式的定义几何体的包，可以按照相同规则进行的处理。基本上，所有的普通包和集合操作函数（见 7.4 和 7.5）都可以作为数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的包进行处理。

若几何操作符返回一个空包，则表示为数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的空包。

在 GeoXACML 策略中〈Rule〉元素中显式定义的所有几何体应使用本标准中同一种编码扩展进行定义。

在 GeoXACML 中，长度的内在单位是米，面积的单位是平方米。相应的，作为函数参数或者函数返回值时，长度或面积的值也是基于 GeoXACML 内部单位。在实际的案例中，如果距离和面积才用不同的测量单位来说明，那么，相应的转化应使用 6.5 定义的函数来完成。

在满足以下条件时，所有定义的函数应返回一个伴随“不确定”状态的 XACML 处理错误信息：

——XML 编码的变量 g 的数据类型是无效的或者不符合 OGC 06-103r4 v1.2.0 中对函数的定义；

——底层函数功能处理返回错误的结果。

另外，当满足以下条件时，任何具有两个变量 g1 和 g2（g1、g2 可以为任意几何类型）的函数应返回一个伴随“不确定”状态的 XACML 处理错误信息：

——根据 OGC 06-103r4 v1.2.0 中的定义，g1 和 g2 的数据类型组合无效；

——g1 和 g2 的坐标参照系定义都显式的给出，但是它们的值是不同的，并且运行时执行不遵守 CRS 转化。

另外，6.4 和 6.5 定义的包和集函数不是空间函数。只有从 6.2～6.3 的空间函数才能用来测试空间条件。

6.2 拓扑函数定义

所有函数都应具有两个数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的变量，并且返回数据类型应为“http://www.w3.org/2001/XMLSchema#boolean”。在以下的定义中，一个几何体可以看作是点的可能无穷集的一个表示。这种表示显然不是无穷的，只是空间范围内的差值算法得到的结果集。相关函数定义如下：

——Contains(g1:Geometry, g2:Geometry):Boolean

此函数应返回一个“True”当且仅当几何体 g2 位于几何体 g1 的封闭区内(边界和内部)。与 Within(g1:Geometry, g2:Geometry)相反。

——Crosses(g1:Geometry, g2:Geometry):Boolean

这个函数应返回一个“True”当且仅当几何体 g1 和 g2 有交集但是任何一个都不包含另一个几何体，交集的维度要小于两个几何体中的任一个。

——Disjoint(g1:Geometry, g2:Geometry):Boolean

这个函数应返回一个“True”当且仅当几何体 g1 和 g2 没有公共点。

——Equals(g1:Geometry, g2:Geometry):Boolean

这个函数应返回一个“True”当且仅当几何体 g1 和 g2 是相等的(在几何上恰好包含相同的点)。

——Intersects(g1:Geometry, g2:Geometry):Boolean

这个函数应返回一个“True”当且仅当几何体 g1 和 g2 至少有一个公共点(与 Disjoint 相反)。

——Overlaps(g1:Geometry, g2:Geometry):Boolean

这个函数应返回一个“True”当且仅当几何体 g1 和 g2 有公共交点但不是所有的点都相交。交集部分的维度与两个几何体的维度相同。

——Touches(g1:Geometry, g2:Geometry):Boolean

这个函数应返回一个“True”当且仅当几何体 g1 和 g2 至少有一个边界公共点，但没有内部公共点。

——Within(g1:Geometry, g2:Geometry):Boolean

这个函数应返回一个“True”当且仅当几何体 g1 空间上在 g2 的内部，也就是说凡是在 g1 上的点也一定在 g2 上。

6.3 几何函数定义

几何函数可分为构造性集合函数、标量几何函数和检查特殊要素函数三类函数集合。其中，构造性集合函数集合中包含了以下函数：

——Buffer(g:Geometry, d:Double):Bag

这个函数应有两个参数，数据类型分别为“urn:ogc:def:dataType:geoxacml:1.0:geometry”和“http://www.w3.org/2001/XMLSchema#double”。

这个函数应返回一个几何值的包，能够描述几何体 g 在距离 d 上的缓冲区域。一个几何体在距离 d 上的缓冲就是一个多边形或者是多边形集，它包含了几何体在距离 d 内的所有的点。变量 d 的度量单位应是米。

——Boundary(g:Geometry):Bag

这个函数应有一个参数，数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”，并返回几何体的包。

这个函数应返回一个几何值的包，该包可以用来描述几何体 g 的组合边界。

——ConvexHull(g:Geometry):Geometry

这个函数应有一个参数，数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”，并返回相同数据类型的值。

这个函数应返回一个能够代表几何体 g 的凸包的几何对象。凸包就是包含几何体的所有点的最小凸多边形。数据类型“点”这种几何体编码的凸包就是点本身。

——Centroid(g:Geometry):Geometry

这个函数应有一个参数，数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”，并返回相同数据类型的值。

这个函数应返回几何体 g 的几何重心的那个点。

——Difference(g1:Geometry, g2:Geometry):Bag

这个函数应有两个参数，数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”，并返回几何体的包。

这个函数应返回一个几何值的包，该包是几何体 g1 和 g2 差的几何闭包。差异就是在 g1 上且不在 g2 上的点的集合。

——SymDifference(g1:Geometry, g2:Geometry):Bag

这个函数应有两个参数，数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”，并返回几何体的包。

这个函数应返回几何值的包，该包是两个几何体对称差的闭包。对称差异就是在 g1 上或者在 g2 上，但不同时在两者之上的点的集合。

——Intersection(g1:Geometry, g2:Geometry):Bag

这个函数应有两个参数，数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”，并返回几何体的包。

这个函数应返回一个几何值的包，该包能够代表几何体 g1 和 g2 的点集交集。

——Union(g1:Geometry, g2:Geometry):Bag

这个函数应有两个参数，数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”，并返回几何体的包。

这个函数应返回一个几何值的包，该包能够代表几何体 g1 和 g2 的点集并集。

标量几何函数集合中包含以下函数：

——Area(g:Geometry):Double

这个函数应有一个参数，数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”，并返回一个数据类型为“http://www.w3.org/2001/XMLSchema＃ double”的值。

这个函数应返回一个能够代表几何体 g 的面积的值。返回值的度量单位应是平方米。如果几何体数据类型是点或者线这个函数应返回零。

——Distance(g1:Geometry, g2:Geometry):Double

这个函数应有两个参数，数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”，并返回一个数据类型为“http://www.w3.org/2001/XMLSchema＃ double”的值。

这个函数应返回几何体 g1 和 g2 上任意两点的最短距离。

因为几何体都是封闭的，所以，几何体上每一个点都是可以确定并找到的，因此，计算两个几何体间的最短距离也是可行的。

——IsWithinDistance(g1:Geometry, g2:Geometry, d:Double):Boolean

这个函数应有三个参数，其中，两个参数的数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”，另外一个参数的数据类型为“http://www.w3.org/2001/XMLSchema＃double”，并返回数据类型为“http://www.w3.org/2001/XMLSchema＃boolean”的值。

这个函数应返回一个“True”当且仅当几何体 g1 和 g2 之间的最小距离小于或等于指定的距

离(单位为米)。

——Length(g:Geometry):Double

这个函数应有一个参数,数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”,并返回数据类型为“http://www.w3.org/2001/XMLSchema# double”的值。

这个函数应返回几何体 g 的长度值,返回值的度量单位应是米。如果几何体数据类型是“点”,函数应返回零。如果几何体数据类型是“多边形”,函数应返回周长。

检查特殊要素函数中的所有函数都应有一个参数,数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”,并返回数据类型为 http://www.w3.org/2001/XMLSchema#boolean 的值。检查特殊要素函数中包含以下函数:

——IsSimple(g:Geometry):Boolean

这个函数应返回一个“True”,当且仅当几何体 g 没有不规则的几何点,如自交、自切。简单的弧线仅在端点相交(只有当它们是闭合时,参考下一函数)。

——IsClosed(g:Geometry):Boolean

这个函数应返回一个“True”,当且仅当弧 g 的起点和终点是同一的。对于一个点来说,点的有限集合或者空的几何体函数应返回一个“True”。面需要一个 3D 的空间来闭合。一般来说,封闭的几何体拥有空的边界。

——IsValid(g:Geometry):Boolean

这个函数应返回一个“True”,当且仅当几何体 g 满足 OGC 06-103r4 v1.2.0 中定义的有效性。

需要说明的是,即使几何体(将被 PDP 处理)毫无疑问是有效的,操作符也会对其进行显式检查。这一点如同 Java 语言中的异常处理一样。Java 定义了能被程序员处理的可检查异常和源代码中异常处理可选的不可检查异常。IsValid 操作符的刻意使用非常类似不可被检查的异常。

6.4 包函数定义

GeoXACML 中对包进行操作的函数。相关函数定义如下:

——GeometryOneAndOnly(b: Bag):Geometry

这个函数应有一个几何体的包作为参数,还应返回一个数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的值。

这个函数应返回包 b 中唯一元素的值。

如果几何包 b 没有一个确切的值,这个函数应返回一个伴有“不确定”状态的 XACML 处理出错信息。

——GeometryBagSize(b: Bag):Integer

这个函数应有一个几何体的包作为参数,并且该包中值的数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”,还应返回数据类型为“http://www.w3.org/2001/XMLSchema#integer”的值。

这个函数应返回包中元素数目。

——GeometryIsIn(g:Geometry, b: Bag):Boolean

这个函数的第一个参数的数据类型应为“urn:ogc:def:dataType:geoxacml:1.0:geometry”第二个参数应是数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的一个包,还应返回类型为“http://www.w3.org/2001/XMLSchema#boolean“的值。

这个函数应返“True”,当且仅当第一个参数与包中的任何值满足匹配函数“urn:ogc:def:function:geoxacml:1.0:geometry-equals”。

——GeometryBag(g * :Geometry):Bag

这个函数应可以有任意个数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的参

数，并返回包含参数值的几何体的包。

这个函数无参时应产生一个数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的空包。

6.5 集合函数定义

本节定义的所有函数均通过消除数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的几何包中的重复元素来模拟对应的集合。集合函数中包含以下函数：

——GeometryBagIntersection(b1: Bag, g2: Bag):Bag

这个函数应有两个参数，均是数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的包。

这个函数应返回一个数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的包，包中包含了满足“urn:ogc:def:function:geoxacml:1.0:geometry-equals”的包 b1 和 b2 共有的元素。并且，在结果中应没有重复元素出现。

——GeometryBagAtLeastOneMemberOf(b1: Bag, b2: Bag):Boolean

这个函数应有两个参数，均是数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的包，还应返回数据类型为“http://www.w3.org/2001/XMLSchema#boolean”的值。

这个函数应返回“True”，当且仅当包 b1 中至少有一个元素与包 g2 的关系满足“urn:ogc:def:function:geoxacml:1.0:geometry-is-in”函数。

——GeometryBagUnion(b1: Bag, b2: Bag):Bag

这个函数应有两个参数，均是数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的包。

这个函数应返回一个数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的包，包中包含了包 b1 和 b2 的所有元素。如同“urn:ogc:def:function:geoxacml:1.0:geometry-equals”中所定义的，应没有重复元素在结果中出现。

——GeometryBagSubset(b1: Bag, b2: Bag):Boolean

这个函数应有两个参数，均是数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的包，并返回数据类型为“http://www.w3.org/2001/XMLSchema#boolean”的值。

这个函数应返回一个“True”，当且仅当包 b1 是包 b2 的一个子集。每一个参数应被认为是去掉了重复元素的。

——GeometrySetEquals(b1: Bag, b2: Bag):Boolean

这个函数应有两个参数，均是数据类型为“urn:ogc:def:dataType:geoxacml:1.0:geometry”的包，并返回数据类型为“http://www.w3.org/2001/XMLSchema#boolean”的值。

这个函数的返回结果应按照以下流程计算：1）对包 b1 和包 b2 计算函数“urn:ogc:def:function:geoxacml:1.0:geometry-bag-subset”；2）对包 b2 和包 b1 的计算函数“urn:ogc:def:function:geoxacml:1.0:geometry-bag-subset”；3）对 1 和 2 的结果计算函数“urn:oasis:names:tc:xacml:1.0:function:and”。

6.6 转化函数的定义

在 GeoXACML 中，长度的内部单位是米，面积的内部单位是平方米。这就意味着基于不同度量单位的长度面积参数在被相应的函数处理（例如：IsWithinDistance 和 Buffer 函数）之前都应转化成米和平方米。这可以通过如下的转换函数来实现：

——ConvertToMetre(d:Double, u:String):Double

这个函数应有一个数据类型为“http://www.w3.org/2001/XML-Schema#double”的参数和

一个数据类型为“http://www.w3.org/2001/XML-Schema#string”的用以表示度量长度单位的参数。这个函数应返回一个数据类型为“http://www.w3.org/2001/XMLSchema#double”的值。

这个函数用于把度量单位为 u 的距离值 d 转化成相应的基于米制的长度。

如果度量单位，如给定的参数 u，不能转化成米，那么这个函数应返回一个“不确定”状态的 XACML 处理出错信息。

——ConvertToSquareMetre(a:Double, u:String):Double

这个函数应有一个数据类型为“http://www.w3.org/2001/XML-Schema#double”的参数和一个数据类型为“http://www.w3.org/2001/XML-Schema#string”的用以表示度量面积单位的参数。这个函数应返回一个数据类型为“http://www.w3.org/2001/XMLSchema#double”的值。

这个函数用于把度量单位为 u 的面积值 a 转化成相应的基于平方米制的面积。

如果度量单位，如给定的参数 u，不能转化成平方米，那么这个函数应返回一个“不确定”状态的 XACML 处理出错信息。

为了避免运行时不必要的转化，宜直接用米和平方米来说明长度和面积。

7 GeoXACML 标识符定义

7.1 概述

任意基于 GeoXACML 的具体实现应按照 GeoXACML 中定义的方式来使用下列标识符的相关属性。以下表格的第二列是第 6 章或者 xacml-2.0-core-spec-os[3] 中使用的函数名字。

7.2 几何体的标识符

应使用表 1 中的标识符来定义“几何体”的几何数据类型。

表 1 GeoXACML 几何体 URN

URN	数据类型
urn:ogc:def:dataType:geoxacml:1.0:geometry	几何体

为了使用明确的编码方案来建立几何数据类型，GeoXACML 在现有的扩展中定义了更多的 URN。

7.3 拓扑函数标识符

为了定义函数来测试拓扑关系，表 2 定义了拓扑函数 URN。

表 2 拓扑函数 URN

URN	函　数
urn:ogc:def:function:geoxacml:1.0:geometry-equals	Equals
urn:ogc:def:function:geoxacml:1.0:geometry-disjoint	Disjoint
urn:ogc:def:function:geoxacml:1.0:geometry-touches	Touches
urn:ogc:def:function:geoxacml:1.0:geometry-crosses	Crosses

表 2（续）

URN	函　　数
urn:ogc:def:function:geoxacml:1.0:geometry-within	Within
urn:ogc:def:function:geoxacml:1.0:geometry-contains	Contains
urn:ogc:def:function:geoxacml:1.0:geometry-overlaps	Overlaps
urn:ogc:def:function:geoxacml:1.0:geometry-intersects	Intersects

7.4　几何函数标识符

为了表达和执行更为复杂的基于空间分析的访问约束，表 3、表 4 和表 5 分别对构造性几何函数 URN、标量几何函数 URN、杂项几何函数 URN 进行了定义。

表 3　构造性几何函数 URN

URN	几何函数
urn:ogc:def:function:geoxacml:1.0:geometry-buffer	Buffer
urn:ogc:def:function:geoxacml:1.0:geometry-boundary	Boundary
urn:ogc:def:function:geoxacml:1.0:geometry-union	Union
urn:ogc:def:function:geoxacml:1.0:geometry-intersection	Intersection
urn:ogc:def:function:geoxacml:1.0:geometry-difference	Difference
urn:ogc:def:function:geoxacml:1.0:geometry-sym-difference	SymDifference
urn:ogc:def:function:geoxacml:1.0:geometry-centroid	Centroid
urn:ogc:def:function:geoxacml:1.0:geometry-convex-hull	ConvexHull

表 4　标量几何函数 URN

URN	几何函数
urn:ogc:def:function:geoxacml:1.0:geometry-distance	Distance
urn:ogc:def:function:geoxacml:1.0:geometry-is-within-distance	IsWithinDistance
urn:ogc:def:function:geoxacml:1.0:geometry-length	Length
urn:ogc:def:function:geoxacml:1.0:geometry-area	Area

表 5　杂项几何函数 URN

URN	几何函数
urn:ogc:def:function:geoxacml:1.0:geometry-is-simple	IsSimple
urn:ogc:def:function:geoxacml:1.0:geometry-is-closed	IsClosed
urn:ogc:def:function:geoxacml:1.0:geometry-is-valid	IsValid

7.5 包含几何体的包函数标识符

为了在包含几何体的包上进行操作，表 6 定义了如下的几何包函数 URN。

表 6 几何包函数 URN

URN	包函数
urn:ogc:def:function:geoxacml:1.0:geometry-one-and-only	GeometryOneAndOnly
urn:ogc:def:function:geoxacml:1.0:geometry-bag-size	GeometryBagSize
urn:ogc:def:function:geoxacml:1.0:geometry-is-in	GeometryIsIn
urn:ogc:def:function:geoxacml:1.0:geometry-bag	GeometryBag

7.6 几何集合函数标识符

表 7 定义了几何集合函数 URN。

表 7 几何集合函数 URN

URN	集合函数
urn:ogc:def:function:geoxacml:1.0:geometry-bag-intersection	GeometryBagIntersection
urn:ogc:def:function:geoxacml:1.0:geometry-at-least-one-member-of	GeometryAtLeastOneMemberOf
urn:ogc:def:function:geoxacml:1.0:geometry-bag-union	GeometryBagUnion
urn:ogc:def:function:geoxacml:1.0:geometry-bag-subset	GeometryBagSubset
urn:ogc:def:function:geoxacml:1.0:geometry-set-equals	GeometrySetEquals

7.7 转化函数标识符

表 8 定义了转化函数 URN。

表 8 转化函数 URN

URN	转化函数
urn:ogc:def:function:geoxacml:1.0:convert-to-metre	ConvertToMetre
urn:ogc:def:function:geoxacml:1.0:convert-to-square-metre	ConvertToSquareMetre

附 录 A
（规范性附录）
GeoXACML 符合性声明表

A.1 概述

本附录针对 GeoXACML 属性、标识符、数据类型、函数定义了两类符合性声明表，标记为“Ⅰ”的为基本符合级，标记为“Ⅱ”的是完全符合级（在“Ⅰ”标记项实现的基础上还应实现的项目）。

GeoXACML 定义了两个符合性等级：

基本符合级（Ⅰ）。所有 PDP 应达到该等级。包含对所有标记“Ⅰ”的定义。

完全符合级（Ⅱ）。在满足基本符合级的基础上，还需要满足所有标记了“Ⅱ”的定义。

A.2 模式组成元素

GeoXACML 没有定义新的模式元素。任意符合 GeoXACML 标准的系统实现应符合 XACML 标准。

A.3 标识符前缀

表 A.1 是为 GeoXACML 保留的标识符前缀。

因为这些标识符前缀是 GeoXACML URN[4] 定义的一部分，所以应在基本符合集中能够实现。

表 A.1 标识符

标识符
urn:ogc:def:dataType:geoxacml:1.0:geometry
urn:ogc:def:function:geoxacml:1.0

任意 GeoXACML 系统实现应能够通过附录 B 中定义的包含了这些标识符前缀的测试。

A.4 算法

GeoXACML 没有定义新的算法。

A.5 状态代码

GeoXACML 没有定义新的状态代码。

A.6 数据类型

表 A.2 是 GeoXACML 的数据类型及其符合性等级。

表 A.2 数据类型

数据类型	符合性等级
urn:ogc:def:dataType:geoxacml:1.0:geometry	I

A.7 函数

表 A.3～表 A.7 分别是 GeoXACML 的拓扑函数、包函数、集合函数、几何函数、转化函数及其符合性等级。

为通过基本符合集，对附录 B 第 2 节中定义的所有测试实例，系统应实现所有标记为“Ⅰ”的函数 URN。

为通过完全符合集，对附录 B 第 2 节中定义的所有测试实例，系统应实现所有标记为“Ⅱ”的函数 URN。

同时，任意通过基本符合集的系统应能够通过 B.4 中定义的测试，该测试应包含表 A.3～表 A.6 所有函数。任意通过完全符合集的系统应能够通过 B.4 中定义的测试，该测试应包含表 A.7 所有函数。

表 A.3 拓扑函数

函数	符合性等级
urn:ogc:def:function:geoxacml:1.0:geometry-equals	I
urn:ogc:def:function:geoxacml:1.0:geometry-disjoint	I
urn:ogc:def:function:geoxacml:1.0:geometry-touches	I
urn:ogc:def:function:geoxacml:1.0:geometry-crosses	I
urn:ogc:def:function:geoxacml:1.0:geometry-within	I
urn:ogc:def:function:geoxacml:1.0:geometry-contains	I
urn:ogc:def:function:geoxacml:1.0:geometry-overlaps	I
urn:ogc:def:function:geoxacml:1.0:geometry-intersects	I

表 A.4 包函数

函数	符合性等级
urn:ogc:def:function:geoxacml:1.0:geometry-one-and-only	I
urn:ogc:def:function:geoxacml:1.0:geometry-bag-size	I
urn:ogc:def:function:geoxacml:1.0:geometry-is-in	I
urn:ogc:def:function:geoxacml:1.0:geometry-bag	I

表 A.5 集合函数

函数	符合性等级
urn:ogc:def:function:geoxacml:1.0:geometry-bag-intersection	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-bag-at-least-one- member-of	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-bag-union	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-bag-subset	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-set-equals	Ⅰ

表 A.6 几何函数

函数	符合性等级
urn:ogc:def:function:geoxacml:1.0:geometry-buffer	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-boundary	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-convex-hull	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-centroid	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-difference	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-sym-difference	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-intersection	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-union	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-area	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-distance	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-is-within-distance	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-length	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-is-simple	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-is-closed	Ⅰ
urn:ogc:def:function:geoxacml:1.0:geometry-is-valid	Ⅰ

表 A.7 转化函数

函数	符合性等级
urn:ogc:def:function:geoxacml:1.0:convert-to-metre	Ⅱ
urn:ogc:def:function:geoxacml:1.0:convert-to-square-metre	Ⅱ

转化函数“urn:ogc:def:function:geoxacml:1.0:convert-to-metre”宜满足从其他可能的长度单位[2]到米的转换。

转化函数“urn:ogc:def:function:geoxacml:1.0:convert-to-square-metre”宜满足从其他可能的面积单位[2]到平方米的转换。

附 录 B
（规范性附录）
GeoXACML 符合性测试

B.1 概述

本附录给出了符合 GeoXACML v1.0 标准的 PDP 应实施的规范细则，用于测试系统实现是否符合 GeoXACML 定义的等级。

任意系统实现是否符合 GeoXACML 标准依赖于其是否符合 XACML 标准。因此，系统首先应能够通过 OASIS Conformance Tests for XACML 1.0 and 1.1 中定义的所有测试。

B.2 分组定义

GeoXACML 有两个不同的测试分组：

——group A：数据类型；

——group B：函数。

每组测试的不同方面在第 7 章和应用扩展中定义。

B.3 符合性测试实例定义

测试套件中的任一测试都针对本标准中特定的限制或要求制定。测试遵照以下模式：

——测试目的：为了测定被测试系统实现是否满足本标准某一特定方面。对于基本符合，只有基本符合集所要求的方面会被添加到测试样例中。对于完全符合，任意基本符合集或完全符合集的要求都会被添加到测试样例中。

——测试方法：一个涉及特定分组的 GeoXACML 实例会被用来做测试，并且期望该系统实现有正确的反映。

——关联：每个测试都会关联要测试的某一个方面。

在本细则中测试的是 GeoXACML 数据类型和函数定义两个分组。对每一组，都应进行包含以下 3 个不同分类的符合性测试：

- “Policy Language Encoding”（PLE）类：在 XML 编码符合 XACML 规范的前提下，确保实例具有正确处理 GeoXACML 定义的地理数据类型和函数的能力。此类测试为基础性测试，应首先进行。
- “Logical and Syntactical Processing”（LSP）类：确保实例具有正确理解 GeoXACML 中定义的函数和地理数据类型的句法的能力，并确保实例能够正确处理依据逻辑定义的地理数据类型和函数。这些测试用例假定 PLE 分类的测试已经完成并且没有错误。
- “Exception Behavior and Processing”（EBP）类：确保实例能够正确进行 GeoXACML 定义的函数和地理数据类型的出错处理。这些测试的一个重要方面是确保系统实现可以正确的交互式处理无效的几何属性值和几何函数结果。这些测试在 PLE 和 LSP 类检测通过的基础上进行。

为协助进行实例检测，针对每个符合性等级和不同的测试分组需要生成不同的测试实例组。

B.4 PLE 符合性测试

表 B.1 给出了所有的 PLE 符合性测试实例。

表 B.1 PLE 符合性测试图

测试实例	描　　述	结　　果
PLE.1	使用 XML 模式有效化机制实现[1]中定义的与 XACML 不同的 GeoXACML 策略文件	验证通过,无错误
PLE.2	PDP 处理 GeoXACML 策略文件	PDP 不报告未知标识符
PLE.3	PDP 使用 AttributeDesignator 处理授权请求	PDP 不报告未知标识符
PLE.4	PDP 使用 AttributeSelector 处理授权请求	PDP 不报告未知标识符

PLE 符合性测试可分为基本符合性测试和完全符合性测试两类。其中,基本符合性测试包含以下内容:

——创建一个 GeoXACML 策略文件,涵盖 Group A 和 Group B 标记为“Ⅰ”的所有方面。

- 测试 PLE.1;
- 测试 PLE.2。

——创建 XACML 授权请求,每个请求至少包含 Group A 中标记为“Ⅰ”的一个方面。

- 测试 PLE.3;
- 测试 PLE.4。

完全符合性测试包含以下内容:

——创建一个 GeoXACML 策略文件,涵盖 Group A 和 Group B 标记为“Ⅱ”的所有方面。

- 测试 PLE.1;
- 测试 PLE.2。

——创建 XACML 授权请求,每个请求至少包含 Group A 中标记为“Ⅱ”的一个方面。

- 测试 PLE.3;
- 测试 PLE.4。

B.5 LSP 符合性测试

表 B.2 给出了所有的 LSP 符合性测试实例。

表 B.2 LSP 符合性测试图

测试实例	描　　述	结　　果
LSP.1	PDP 处理 GeoXACML 策略文件,对没有错误的例子验证返回结果	见定义

LSP 符合性测试可分为基本符合性测试和完全符合性测试两类。其中,基本符合性测试包含以下内容:

——对 Group B 中标记为“Ⅰ”的各个方面,赋予有效的 GroupA 参数,并执行测试 LSP.1。

完全符合性测试包含以下内容:

——对 Group B 中标记为“Ⅱ”的各个方面,赋予有效的 GroupA 参数,并执行测试 LSP.1。

B.6 EBP 符合性测试

表 B.3 给出了所有的 EBP 符合性测试实例。

表 B.3 EBP 符合性测试图

测试实例	描　　述	结　　果
EBP.1	PDP 处理合理的授权决定要求	PDP 应不报错
EBP.2	PDP 处理无效的授权决定要求	PDP 应报告处理出错
EBP.3	PDP 处理合理的策略文档	PDP 应不报错
EBP.4	PDP 处理不合理的策略文档	PDP 应报告处理出错

EBP 符合性测试可分为基本符合性测试和完全符合性测试两类。其中，基本符合性测试包含以下内容：

——对于 Group A 的测试：对 Group A 中标记为“Ⅰ”的各个方面执行测试 EBP.1、EBP.2、EBP.3 和 EBP.4。

——对于 Group B 的测试：对 Group B 中标记为“Ⅰ”的各个方面执行测试 EBP.3 和 EBP.4。

完全符合性测试包含以下内容：

——对于 Group A 的测试：对 Group A 中标记为“Ⅱ”的各个方面执行测试 EBP.1、EBP.2、EBP.3 和 EBP.4。

——对于 Group B 的测试：对 Group B 中标记为“Ⅱ”的各个方面执行测试 EBP.3 和 EBP.4。

参 考 文 献

[1] OASIS, eXtensible Access Control Markup Language (XACML) Version 2.0-Policy XML Schema: access_control-xacml-2.0-policy-schema-os.xsd

[2] National Institute of Standards and Technology (NIST), NIST Guide to SI Units: B.9 Factors for units listed by kind of quantity or field of science, http://physics.nist.gov/Pubs/SP811/appenB9.html

[3] OASIS, eXtensible Access Control Markup Language (XACML) Version 2.0, 1 Feb 2005, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[4] OGC, Definition identifier URNs in OGC namespace, Version 1.1.0, 2006-08-08, http://portal.opengeospatial.org/files/? artifact_id=16339

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 鉴别与授权
地理空间可扩展访问控制置标语言
GB/T 30280—2013
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:400-168-0010
010-68522006
2014 年 5 月第一版
*
书号:155066·1-49178

GB/T 30280-2013