



# 中华人民共和国国家标准

GB/T 30281—2013

---

## 信息安全技术 鉴别与授权 可扩展访问控制标记语言

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

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 .....	V
引言 .....	VI
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 缩略语 .....	3
5 XACML 概述 .....	3
5.1 概述 .....	3
5.2 需求 .....	3
5.3 规则和策略组合 .....	4
5.4 组合算法 .....	4
5.5 多主体 .....	5
5.6 基于主体和资源属性的策略 .....	5
5.7 多值属性 .....	5
5.8 基于资源内容的策略 .....	5
5.9 操作符 .....	5
5.10 策略分布 .....	6
5.11 策略索引 .....	6
5.12 抽象层 .....	6
5.13 随同策略实施一起执行的动作 .....	6
6 模型 .....	6
6.1 数据流模型 .....	6
6.2 XACML 上下文 .....	7
6.3 策略语言模型 .....	8
7 策略语法 .....	10
7.1 <PolicySet>元素 .....	10
7.2 <Description>元素 .....	12
7.3 <PolicySetDefaults>元素 .....	12
7.4 <XpathVersion>元素 .....	12
7.5 <Target>元素 .....	12
7.6 <Subjects>元素 .....	13
7.7 <Subject>元素 .....	13
7.8 <SubjectMatch>元素 .....	14
7.9 <Resources>元素 .....	14
7.10 <Resource>元素 .....	14
7.11 <ResourceMatch>元素 .....	15

7.12	〈Actions〉元素	15
7.13	〈Action〉元素	15
7.14	〈ActionMatch〉元素	16
7.15	〈Environments〉元素	16
7.16	〈Environment〉元素	17
7.17	〈EnvironmentMatch〉元素	17
7.18	〈PolicySetIdReference〉元素	17
7.19	〈PolicyIdReference〉元素	18
7.20	VersionType 简单类型	18
7.21	VesionMatchType 简单类型	18
7.22	〈Policy〉元素	19
7.23	〈PolicyDefaults〉元素	20
7.24	〈CombinerParameters〉元素	20
7.25	〈CombinerParameter〉元素	21
7.26	〈RuleCombinerParameters〉元素	21
7.27	〈PolicyCombinerParameters〉元素	22
7.28	〈PolicySetCombinerParameters〉元素	22
7.29	〈Rule〉元素	23
7.30	EffectType 简单类型	23
7.31	〈VariableDefinition〉元素	23
7.32	〈VariableReference〉元素	24
7.33	〈Expression〉元素	24
7.34	〈Condition〉元素	25
7.35	〈Apply〉元素	25
7.36	〈Function〉元素	25
7.37	AttributeDesignatorType 复合类型	26
7.38	〈SubjectAttributeDesignator〉元素	27
7.39	〈ResourceAttributeDesignator〉元素	27
7.40	〈ActionAttributeDesignator〉元素	28
7.41	〈EnvironmentAttributeDesignator〉元素	28
7.42	〈AttributeSelector〉元素	28
7.43	〈AttributeValue〉元素	29
7.44	〈Obligations〉元素	30
7.45	〈Obligation〉元素	30
7.46	〈AttributeAssignment〉元素	31
8	上下文语法	31
8.1	〈Request〉元素	31
8.2	〈Subject〉元素	32
8.3	〈Resource〉元素	32
8.4	〈ResouceContent〉元素	33
8.5	〈Action〉元素	33
8.6	〈Environment〉元素	33
8.7	〈Attribute〉元素	34

8.8	〈AttributeValue〉元素	34
8.9	〈Response〉元素	35
8.10	〈Result〉元素	35
8.11	〈Decision〉元素	36
8.12	〈Status〉元素	36
8.13	〈StatusCode〉元素	37
8.14	〈StatusMessage〉元素	37
8.15	〈StatusDetail〉元素	37
8.16	〈MissingAttributeDetail〉元素	38
9	功能需求	38
9.1	概述	38
9.2	策略执行点	38
9.3	属性评估	39
9.4	表达式评估	40
9.5	算术评估	41
9.6	匹配评估	41
9.7	目标评估	42
9.8	变量引用评估	43
9.9	条件评估	44
9.10	规则评估	44
9.11	策略评估	44
9.12	策略集评估	45
9.13	有层次的资源	45
9.14	授权决策	45
9.15	义务	46
9.16	异常处理	46
10	XACML 扩展点	46
10.1	可扩展的 XML 属性类型	46
10.2	结构化属性	47
11	安全和隐私	47
11.1	概述	47
11.2	威胁模型	47
11.3	安全措施	49
12	符合性	51
12.1	介绍	51
12.2	符合性列表	51
附录 A (规范性附录)	数据类型和函数	61
附录 B (规范性附录)	XACML 标识符	76
附录 C (规范性附录)	组合算法	80
参考文献		89

## 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。

本标准主要起草人:冯登国、徐震、张敏、翟征德、王雅哲、高志刚、张凡。

## 引 言

如何实现大规模分布式应用中的信息资源的受控共享,实现基于策略的安全管理已成为信息安全领域关注的重点之一。目前多数分布式应用仍然独立定义自己的安全策略并实施资源访问控制,不仅无法获得一个完整的安全策略实施视图,而且安全策略的维护代价高,可靠性缺乏足够保障。

本标准定义一种通用的可扩展的访问控制策略标记语言 XACML,支持多种访问控制策略类型,允许用户自定义策略扩展,允许用户以一种实现无关的方式定义系统的资源保护策略并控制资源访问控制决策的逻辑过程,实现安全策略定义形式和访问判定过程标准化。

# 信息安全技术 鉴别与授权 可扩展访问控制标记语言

## 1 范围

本标准规定了可扩展访问控制标记语言(XACML)的数据流模型、语言模型和语法。  
本标准适用于大规模分布式应用中资源统一访问控制策略语言的编写与分析。

## 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。

IEEE 754 浮点运算标准(Standard for Floating-point Arithmetic)

IETF RFC 822 电子邮件的标准格式(Standard for the Format of Arpa Internet Text Messages)

IETF RFC 2253 轻型目录访问协议(v3);UTF-8 字符串表示辨别名(Lightweight Directory Access Protocol (v3);UTF-8 String Representation of Distinguished Names)

IETF RFC 2396 统一资源标识符:基本语法(Uniform Resource Identifiers (URI): Generic Syntax)

IETF RFC 2732 文本 IPv6 地址在 URL 上的格式(Format for Literal IPv6 Addresses in URL's)

IETF RFC 3280 X.509 PKI 证书和 CRL 简况(Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)

W3C XQuery1.0 和 XPath 2.0 函数与操作符(XQuery 1.0 and XPath 2.0 Functions and Operators)

W3C XML 模式,第 1 部分和第 2 部分(XML Schema, parts 1 and 2)

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**属性 attribute**

在谓词和目标中用于描述主体、资源、动作和环境的特征。

### 3.2

**授权决策 authorization decision**

PDP 依据适用策略产生的评估结果,该结果返回至 PEP。

### 3.3

**上下文 context**

决策请求和授权决策的规范表述。

### 3.4

**上下文处理器 context handler**

将决策请求从原始格式的决策请求转换成 XACML 规范形式,并将授权决策从 XACML 规范形式