ICS 35.040
L 80

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

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