ICS 35.040
L 80

中华人民共和国国家标准

GB/T 29242—2012

信息安全技术　鉴别与授权　安全断言置标语言

Information security technology—Authentication and authorization—Security assertion markup language

2012-12-31 发布　　2013-06-01 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

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 鉴别与授权
安全断言置标语言
GB/T 29242—2012
*
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(100013)
北京市西城区三里河北街16号(100045)
网址:www.gb168.cn
服务热线:010-51780168
010-68522006
2013年5月第一版
*
书号:155066·1-46985

目　　次

前　言

本标准依据 GB/T 1.1—2009 给出的规则起草，在制定过程中参考了信息标准促进组织(OASIS：Organization for the Advancement of Structured Information Standards)的 saml-core-2.0-os。

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、工业和信息化部电信研究院。

本标准主要起草人：陈驰、冯登国、付艳艳、张立武、荆继武、聂秀英、毕立波、薛宁、江浩洁、武静。

引　言

近年来，越来越多的信息系统通过 Web 服务、门户和集成化应用程序等方式实现互联，彼此间的安全信息共享需求日益强烈。但在互联网跨安全领域应用场景中，缺乏关于认证、属性和授权信息传输格式和协议的规范，信息安全产品之间互操作困难的情况，仍没有得到很好的解决。本标准通过定义一整套严格的、遵从 XML 编码格式的、关于安全断言的语法和语义规范以及标准的协议集合来缓解这种状况。

本标准参考了结构化信息标准促进组织（OASIS）的文件 Security Assertion Markup Language（SAML）v2.0。在原文件的基础上增加了“术语和定义”部分，增加了对标准范围的说明，修改了原文件的简介部分并增设了附录说明。同时新增了协议关系图说明各 SAML 协议间的关系。

信息安全技术　鉴别与授权
安全断言置标语言

1　范围

本标准定义了一系列遵从 XML 编码格式的关于安全断言的语法、语义规范、系统实体间传递和处理 SAML 断言的协议集合和 SAML 系统管理相关的处理规则。

本标准适用于在互联网跨安全域应用场景中，身份鉴别，认证与授权服务的开发、测试、评估和采购。

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。

ISO/IEC 13568:2002　信息技术　Z 形式规范注释　语法、形式系统和语义学(Information technology—Z formal specification notation—Syntax, type system and semantics)

RFC 1510 Kerberos　网络认证请求器(V5)(The Kerberos Network Authentication Service(V5))

RFC 2253　轻量级目录访问控制(V3)(Lightweight Directory Access Protocol(V3))

RFC 2396　统一资源标识：通用语法(Uniform Resource Identifiers (URI): Generic Syntax)

RFC 2822　因特网消息格式(Internet Message Format)

RFC 3513　IPV6 地址结构(Internet Protocol Version 6 (IPv6) Addressing Architecture)

3　术语和定义

下列术语和定义适用于本文件。

3.1

断言　assertion

由 SAML 权威生成的对于主体认证行为的结果，包括与主体相关的属性信息或主体可使用的授权信息等数据。

3.2

鉴别　authentication

验证实体所声称的身份的动作。

3.3

授权　authorization

给予权利，包括访问权的授予。

3.4

绑定，协议绑定　binding, protocol binding

将一个关于协议消息和消息交换模式的标准映射到另一个协议的具体形式标准。

注：将 SAML 中的〈AuthnRequest〉消息映射到 HTTP 就是绑定的一个例子。下文中，在 SAML 上每个绑定都以“SAML xxx binding”的格式命名。