ICS 35.040
L 80

中华人民共和国国家标准

GB/T 35287—2017

信息安全技术　网站可信标识技术指南

Information security technology—
Guidelines of trusted identity technology for website

2017-12-29 发布　　2018-07-01 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

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。

本标准主要起草单位:上海格尔软件股份有限公司、上海凭安网络科技有限公司、北京奇虎科技有限公司、腾讯科技(北京)有限公司、西安西电捷通无线网络通信股份有限公司(无线网络安全技术国家工程实验室)、北京天威诚信电子商务服务有限公司、上海市数字证书认证中心有限公司、中金金融认证中心有限公司、北京数字认证股份有限公司、北龙中网(北京)科技有限责任公司、上海交通大学、四川大学、北京金山安全软件有限公司。

本标准主要起草人:杨茂江、韩洪慧、任伟、石晓虹、叶枫、徐骥、黄振海、杜志强、胡亚楠、郝萱、崔久强、赵宇、付大鹏、高宁、范磊、陈兴蜀、王海舟、张志和、陶思男。

引　言

随着互联网快速发展，信息化已经深入社会的各个领域，并且发挥愈来愈重要的作用，同时安全问题对互联网行业的威胁也越来越大，其中假冒和钓鱼网站的危害尤为严重，如何保证网站身份真实性，有效抵制假冒、钓鱼网站已经成为国家信息系统安全建设急需解决的重要问题。

本标准定义了一种基于我国自主密码算法、可以承载网站真实信息的可信标识体系框架，并对可信标识对象、可信标识对象管理、可信标识对象获取与验证、数据格式与接口等内容进行了规范，旨在推动基于国家自主密码算法的互联网信任体系的建立。网站可信标识以自主密码技术为基础，以开放和可扩展的方式建立全新的网站认证体系和管理体系。

信息安全技术　网站可信标识技术指南

1　范围

本标准规定了用于识别网站真实信息的可信标识体系框架，并对可信标识对象、可信标识对象管理、可信标识对象获取与验证、数据格式与接口等内容进行了规范。

本标准适用于可信标识的管理系统、可信标识验证工具等系统的开发、实现和测评。

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 16262(所有部分)　信息技术　抽象语法记法一(ASN.1)

GB/T 16264.8—2005　信息技术　开放系统互连　目录　第8部分：公钥和属性证书框架

GB 17859—1999　计算机信息系统　安全保护等级划分准则

GB/T 18336(所有部分)　信息技术　安全技术　信息技术安全评估准则

GB/T 19713—2005　信息技术　安全技术　公钥基础设施　在线证书状态协议

GB/T 25069—2010　信息安全技术　术语

GM/T 0003(所有部分)　SM2椭圆曲线公钥密码算法

GM/T 0004—2012　SM3密码杂凑算法

RFC 1777　LDAP轻量级目录访问协议(Lightweight directory access protocol)

3　术语和定义

GB 17859—1999、GB/T 18336和GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

网站可信标识　website trusted identity

具有唯一性、防伪造及可鉴别，用于描述网站真实信息的一段数据，简称可信标识。

3.2

标识权威机构　identity authority

负责网站可信标识整个生命周期(注册申请、签发、发布、撤销等)管理的机构。

3.3

可信应用　trusted application

支持网站可信标识验证及展示的应用，包括浏览器、搜索引擎、即时通讯软件等。

4　缩略语

下列缩略语适用于本文件。

IA：标识权威机构(Identity Authority)

IRL：标识撤销列表(Identity Revocation List)

HTTP：超文本传输协议(Hypertext Transfer Protocol)