ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.3—2016/ISO/IEC 9798-3:1998
代替 GB/T 15843.3—2008

信息技术　安全技术　实体鉴别 第3部分:采用数字签名技术的机制

Information technology—Security techniques—Entity authentication—Part 3:Mechanisms using digital signature techniques

(ISO/IEC 9798-3:1998,IDT)

2016-04-25 发布　　2016-11-01 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

GB/T 15843《信息技术　安全技术　实体鉴别》目前分为五个部分：

——第1部分：概述；

——第2部分：采用对称加密算法的机制；

——第3部分：采用数字签名技术的机制；

——第4部分：采用密码校验函数的机制；

——第5部分：采用零知识技术的机制。

本部分为GB/T 15843的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 15843.3—2008《信息技术　安全技术　实体鉴别　第3部分：采用数字签名技术的机制》。本部分与GB/T 15843.3—2008相比，主要技术变化如下：

——增补了引入在线可信第三方的鉴别机制(见第6章)；

——增补了OID和ASN.1语法(见附录B)。

其中，对GB/T 15843.3—2008修改时涉及的有关章条的信息如下：

修改项号	GB/T 15843.3—2008章条号	修改说明
1	第1章	替换了第1章的第三段文字
2	第3章	在第3章最后增加了三个术语说明
3		在第5章的后面增加第6章
4	附录A	替换了附录A的第一段文字
5		在附录A的后面增加附录B

本部分使用翻译法等同采用ISO/IEC 9798-3:1998《信息技术　安全技术　实体鉴别　第3部分：采用数字签名技术的机制》及其Amd.1:2010《信息技术　安全技术　实体鉴别　第3部分：采用数字签名技术的机制　第1号修改单：引入在线可信第三方的鉴别机制》，仅有编辑性修改。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分主要起草单位：西安西电捷通无线网络通信股份有限公司、国家密码管理局商用密码检测中心、信息安全国家重点实验室、中国电子技术标准化研究所、国家无线电监测中心检测中心、西安电子科技大学、西安邮电大学、广州杰赛科技股份有限公司、深圳市明华澳汉科技股份有限公司、中国信息安全认证中心、国家信息安全工程技术研究中心、国家计算机网络应急技术处理协调中心、国家信息技术安全研究中心、公安部第一研究所、工业和信息化部通信计量中心、公安部信息安全等级保护评估中心、国防科技大学、北京市政务网络管理中心、重庆邮电大学、宇龙计算机通信科技(深圳)有限公司、中国人民大学、中国人民解放军信息安全测评认证中心、中国电信集团公司、国家信息中心、北京大学深圳研究生院、中国电力科学研究院、北京中电华大电子设计有限责任公司、东南大学、中国移动通信集团设计院有限公司、中国人民解放军信息工程大学、江南计算技术研究所、北京邮电大学、上海龙照电子有限公司、北京五龙电信技术公司、北京网贝合创科技有限公司、深圳市宏电技术股份有限公司、北大方正集团公司、海尔集团公司、北京广信融科技术有限公司、北京六合万通微电子技术有限公司、弘浩明传科技(北京)有限公司、北京城市热点资讯有限公司、北京华安广通科技发展有限公司、迈普通信技术有限公司、长春吉大正元信息技术股份有限公司、清华大学、北京天一集成科技有限公司、桂林电子科技大学、西安

立人科技股份有限公司、宽带无线IP标准工作组、WAPI产业联盟。

本部分主要起草人：黄振海、赖晓龙、李大为、冯登国、宋起柱、铁满霞、曹军、李建东、林宁、舒敏、朱志祥、陈晓桦、郭晓雷、李京春、余亚莉、王育民、张变玲、肖跃雷、高波、高昆仑、潘峰、胡亚楠、蒋庆生、肖雳、朱建平、贾焰、施伟年、李琴、李广森、吴亚非、梁朝晖、梁琼文、罗旭光、龙昭华、沈凌云、张伟、徐平平、马华兴、高峰、仇洪冰、朱跃生、王雅辉、兰天、王志坚、杜志强、张国强、田小平、田辉、张永强、寿国梁、毛立平、曹竹青、郭志刚、高宏、韩康、王钢、白国强、陈志峰、李建良、李大伟、王立仁、高原、岳林、井经涛。

本部分所代替标准的历次版本发布情况为：

——GB/T 15843.3—1998、GB/T 15843.3—2008。

引　言

GB/T 15843 的本部分定义了采用数字签名技术的实体鉴别机制，分为单向鉴别和相互鉴别两种。其中单向鉴别按照消息传递的次数，又分为一次传递鉴别和两次传递鉴别；相互鉴别根据消息传递的次数，分为两次传递鉴别、三次传递鉴别、两次传递并行鉴别、五次传递鉴别。

由于签名所使用的证书的分发方式超出本部分范围，证书的发送在所有的机制中是可选的。

本部分凡涉及密码算法的相关内容，按国家有关法规实施。

本文件的发布机构提请注意，声明符合本文件时，可能涉及第 6 章与“一种实体双向鉴别方法”“一种基于可信第三方的实体双向鉴别方法及其系统”等相关的专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构保证，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件发布机构备案。相关信息可通过以下联系方式获得：

专利权人：西安西电捷通无线网络通信股份有限公司

地址：西安市高新区科技二路 68 号西安软件园秦风阁 A201

联系人：刘长春

邮政编码：710075

电子邮件：ipri@iwncomm.com

电话：029-87607836

传真：029-87607829

网址：http://www.iwncomm.com

请注意除了上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

信息技术　安全技术　实体鉴别
第3部分:采用数字签名技术的机制

1　范围

GB/T 15843的本部分规定了采用数字签名技术的实体鉴别机制。有两种鉴别机制是单个实体的鉴别(单向鉴别),其余是两个实体的相互鉴别机制。

本部分中规定的机制采用诸如时间戳、序号或随机数等时变参数,防止先前有效的鉴别信息以后又被接受或者被多次接受。

如果采用时间戳或序号,则单向鉴别只需一次传递,而相互鉴别则需两次传递。如果采用随机数的挑战-响应方法,单向鉴别需两次传递,相互鉴别则需三次、两次传递并行或五次传递(依赖于所采用的机制)。

本部分适用于所有有鉴别需求的应用和设备。

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 15843.1—2008　信息技术　安全技术　实体鉴别　第1部分:概述(ISO/IEC 9798-1:1997,IDT)

GB 15851—1995　信息技术　安全技术　带消息恢复的数字签名方案(idt ISO/IEC 9796:1991)

GB/T 16263.1—2006　信息技术　ASN.1　编码规则　第1部分:基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)规范(ISO/IEC 8825-1:2002,IDT)

ISO/IEC 14888(所有部分)　信息技术　安全技术　带附录的数字签名(Information technology—Security techniques—Digital signatures with appendix)

3　术语、定义和符号

GB/T 15843.1—2008界定的术语、定义以及下列符号适用于本文件。

I_A:实体A的身份标识,可以是A或者CertA

I_B:实体B的身份标识,可以是B或者CertB

ResX:实体X的证书验证结果或实体X的公钥

4　要求

本部分规定的鉴别机制中,待鉴别的实体通过表明它拥有某个私有签名密钥来证实其身份。这要由实体使用其私有签名密钥对特定数据签名来完成。该签名能够由使用该实体的公开验证密钥的任何实体来验证。

鉴别机制有下述要求:

a)　验证方应拥有声称方的有效公开密钥;