ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15843.2—2017/ISO/IEC 9798-2:2008
代替 GB/T 15843.2—2008

信息技术　安全技术　实体鉴别 第2部分:采用对称加密算法的机制

Information technology—Security techniques—Entity authentication—Part 2:Mechanisms using symmetric encipherment algorithms

(ISO/IEC 9798-2:2008,IDT)

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

GB/T 15843《信息技术　安全技术　实体鉴别》目前已经或计划发布以下部分：

——第1部分：总则；

——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；

——第6部分：采用人工数据传递的机制。

本部分为GB/T 15843的第2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 15843.2—2008《信息技术　安全技术　实体鉴别　第2部分：采用对称加密算法的机制》，与GB/T 15843.2—2008相比，主要变化如下：

——在第3章中，增加了除引用ISO/IEC 9798-1:1997中定义的术语以外的七个术语的描述；

——将原第3章中的“符号”独立为第4章“符号和缩略语”；

——在第5章“要求”中增加了验证时变参数的要求；

——增加了两个附录：附录A和附录C。

本部分使用翻译法等同采用ISO/IEC 9798-2:2008《信息技术　安全技术　实体鉴别　第2部分：采用对称加密算法的机制》。

与本部分中规范性引用的国际文件中有一致性对应关系的我国文件如下：

——GB/T 15843.1—2017　信息技术　安全技术　实体鉴别　第1部分：总则(ISO/IEC 9798-1:2010，IDT)

本部分做了下列编辑性修改：

——纳入ISO/IEC 9798-2:2008 TECHNICAL CORRIGENDUM 3:2013的内容；

——并列项编号由“(1)、(2)……”改为“a)、b)……”。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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。

本部分起草单位：中国科学院数据与通信保护研究教育中心、北京江南天安科技有限公司、普华诚信信息技术有限公司。

本部分主要起草人：夏鲁宁、张琼露、荆继武、朱家雄、谢超。

本部分所代替标准的历次版本发布情况为：

——GB/T 15843.2—1997、GB/T 15843.2—2008。

引　言

本部分等同采用 ISO/IEC 9798-2:2008 及其勘误文件 ISO/IEC 9798-2:2008 TECHNICAL CORRIGENDUM 3,它是由 ISO/IEC 联合技术委员会 JTC1(信息技术)的分委员会 SC 27(信息安全技术)起草的。

本部分规定了采用对称加密算法的实体鉴别机制,包括单向鉴别机制和相互鉴别机制,不涉及可信第三方的鉴别机制和涉及可信第三方的鉴别机制,并给出了对这些鉴别机制的要求。

在不涉及可信第三方的情况下,单向鉴别机制包括一次传递鉴别和两次传递鉴别两种,相互鉴别机制包括两次传递鉴别和三次传递鉴别两种。如果涉及可信第三方,相互鉴别机制则需要进行四次或者五次传递。

本部分凡涉及密码算法的相关内容,按国家有关法规实施。

信息技术　安全技术　实体鉴别
第2部分:采用对称加密算法的机制

1　范围

GB/T 15843的本部分规定了采用对称加密算法的实体鉴别机制。其中有四种是两个实体间无可信第三方参与的鉴别机制,这四种机制中有两种是由一个实体针对另一个实体的单向鉴别,另两种是两个实体相互鉴别。其余的机制都要求有一个可信第三方参与,以便建立公共的秘密密钥,实现相互或单向的实体鉴别。

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。

如果没有可信第三方参与同时又采用时间戳或序号,则对于单向鉴别只需传递一次信息,而要实现相互鉴别需传送两次。如果没有可信第三方参与同时又采用使用随机数的挑战—响应方法时,单向鉴别需传递两次信息,而相互鉴别则需传递三次。如果有可信第三方参与,则一个实体与可信第三方之间的任何一次附加通信都需要在通信交换中增加两次传递。

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 9798-1　信息技术　安全技术　实体鉴别　第1部分:总则(Information technology—Security techniques—Entity authentication—Part 1:General)

3　术语和定义

ISO/IEC 9798-1界定的以及下列术语和定义适用于本文件。

3.1

可鉴别的加密　authenticated encryption

通过一种密码算法对数据进行的(可逆)变换,所产生的密文一旦被未授权实体替换,就可被检测出来,也就是说,它提供了数据机密性,数据完整性和数据起源鉴别的保护。

[ISO/IEC 19772:2009]

3.2

密文　ciphertext

经过变换的数据,以隐藏其信息内容。

[ISO/IEC 10116:2006]

3.3

声称方　claimant

身份可被鉴别的实体,包括其功能以及在鉴别交互中必要的私有数据。

[ISO/IEC 9798-5:2004]