ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 15843.2—20XX/ISO/IEC 9798-2:2019
代替 GB/T 15843.2—2017

信息安全技术 实体鉴别
第 2 部分 采用可鉴别加密技术的机制

Information security techniques—Entity authentication—

Part 2: Mechanisms using authenticated encryption

（ISO/IEC 9798-2: 2019,MOD）

（征求意见稿）

（本稿完成日期：2023 年 3 月 7 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分:标准化文件的结构和起草规则》、GB/T 1.2—2020《标准化工作导则　第 2 部分:以 ISO/IEC 标准化文件为基础的标准化文件起草规则》的规定起草。

本文件是GB/T 15843《信息技术　安全技术　实体鉴别》的第2部分。GB/T 15843已经发布了以下部分：

——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：使用零知识技术的机制；

——第6部分：采用人工数据传递的机制。

本文件代替GB/T 15843.2—2017《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—2017相比，主要技术变化如下：

a) 更改了标准名称,由“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”，改为“信息安全技术　实体鉴别　第2部分：采用可鉴别加密技术的机制”，与标准正文内容以及国际标准ISO/IEC 9798-2:2019的名称保持一致；

b) 删掉了“范围”中关于时变参数、信息传递次数的说明，将其纳入第5章（见第5章，2017年版的第1章）；

c) 用等同采用国际标准的GB/T 15843.1代替了ISO/IEC 9798-1；增加了规范性引用文件GB/T 36624（见第2、3章，2017版的第2、3章）、GB/T 25069（见第2、3章）；

d) 增加了术语“验证方”（见3.4），更改了术语“可鉴别的加密”（见3.1,2017年版的3.1）、“密文”（见3.2,2017年版的3.2）、“声称方”（见3.3,2017年版的3.3）、“时间戳”（见3.5,2017年版的3.6）、“可信第三方”（见3.6,2017年版的3.7）的定义，删除了术语“消息鉴别码”（见2017年版的3.4）、“消息鉴别码算法”（见2017年版的3.5）；

e) 增加了符号 “SID^{i}_{m}”（见第4章、第6章、第7章、第8章、附录A），删掉了“X‖Y”原有的“注”（见2017年版的第4章）；

f) 增加了“总则”，将鉴别机制中与时变参数、信息传递次数等相关的说明内容纳入此部分，同时补充了对附录的说明（见第5章，2017年版的第5章）；

g) 更改了“要求”中关于“对称加密”相关的说法，替换为“可鉴别的加密”（见第6章，2017年版的第5章）；

h) 更改了关于“可信第三方”的描述，替换为“在线可信第三方”（见第7章、第8章，2017年版的第6章、第7章）；

i) 更改了各类机制的代号，用英文缩写代替原有数字（见第7章、第8章、附录A、附录C，2017年版的第6章、第7章、附录A、附录C）；

j) 更改了“对象标识符”（见附录A,2017年版的附录A），删掉了“符合ASN.1基本编码规则（BER）的编码示例”（见2017年版的A.3）；

k) 增加了对“文本字段的使用”的相关说明（见附录B）；

l) 增加了参考文献“GB/T 15843.5”、“GB/T 16263.1”、“GB/T 17901.1”、“GB/T 32907”（见“参考文献”）。

本文件修改采用ISO/IEC 9798-2:2019《信息技术 安全技术 实体鉴别 第2部分：采用可鉴别加密技术的机制》。

本文件与ISO/IEC 9798-2:2019的技术性差异及原因如下：

——关于规范性引用文件，本文件做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第2章“规范性引用文件”中，具体调整如下：

· 用等同采用国际标准的GB/T 15843.1代替了ISO/IEC 9798-1（见第2、3章）；

· 用修改采用国际标准的GB/T 36624代替了ISO/IEC 19772（见第2、3章）；

——第3章中，直接采用现行国家标准中已定义的术语定义（见第3章）。

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。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：北京数字认证股份有限公司、中国科学院大学、普华诚信信息技术有限公司、飞天诚信科技股份有限公司、格尔软件股份有限公司、浙江大华技术股份有限公司、中国科学院软件研究所、陕西省信息化工程研究院、郑州信大捷安信息技术股份有限公司、北京国脉信安科技有限公司、启明星辰信息技术集团股份有限公司、北京山石网科信息技术有限公司、北京信安世纪科技股份有限公司、公安部第三研究所、华为技术有限公司、兴唐通信科技有限公司、鼎铉商用密码测评技术（深圳）有限公司、河南中科安永科技有限公司、北京时代新威信息技术有限公司、西安得安信息技术有限公司、安徽科测信息技术有限公司、长扬科技(北京)股份有限公司。

本文件主要起草人：夏鲁宁、张琼露、荆继武、朱家雄、谢超……。

本文件及其所代替文件的历次版本发布情况为：

——1997年首次发布为GB/T 15843.2—1997，2008年第一次修订，2017年第二次修订；

——本次为第三次修订。

引　言

GB/T 15843系列标准确定了6种实体鉴别机制，由6部分组成：

——第1部分：总则。目的在于指明实体鉴别机制中的鉴别模型和一般性约束要求,并基于此验证实体身份真实性。

——第2部分：采用可鉴别加密技术的机制。目的在于规定采用可鉴别的加密技术实现实体鉴别的机制。

——第3部分：采用数字签名技术的机制。目的在于规定采用数字签名技术的实体鉴别机制。

——第4部分：采用密码校验函数的机制。目的在于规定采用密码校验函数的实体鉴别机制。

——第5部分：使用零知识技术的机制。目的在于说明使用零知识技术的实体鉴别机制。

——第6部分：采用人工数据传递的机制。目的在于规定在设备之间基于人工数据传递进行实体鉴别的机制。

GB/T 36624—2018《信息技术　安全技术　可鉴别的加密机制》修改采用ISO/IEC 19772:2009，规定了五种可鉴别的加密机制。本文件基于GB/T 36624，修改采用ISO/IEC 9798-2:2019，规定了6种采用可鉴别的加密技术实现实体鉴别的机制，以指导基于可鉴别的加密实现的实体鉴别系统、产品或服务的建设和研发，为密码检测机构评估密码产品实体鉴别协议的合规性做依据。

信息安全技术 实体鉴别
第2部分：采用可鉴别加密技术的机制

1 范围

本文件规定了采用可鉴别的加密技术实现实体鉴别的机制。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在线可信第三方参与，以便建立公共的秘密密钥，实现单向或相互的实体鉴别。附录A定义了本文件指定机制的对象标识符。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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—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）

GB/T 25069—2022 信息安全技术 术语

GB/T 36624—2018 信息技术 安全技术 可鉴别的加密机制（ISO/IEC 19772:2009, MOD）

3 术语和定义

GB/T 15843.1—2017、GB/T 25069—2022、GB/T 36624—2018 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

一种可逆的数据转换，利用密码算法产生数据对应的密文，非授权实体无法在不被发现的情况下对该密文进行修改，同时提供了数据保密性、数据完整性与数据源鉴别。

[来源：GB/T 36624—2018,3.1]

3.2

密文 ciphertext

采用密码算法，经过变换将其信息内容隐藏起来的数据。

[来源：GB/T 25069—2022,3.388]

3.3

声称方 claimant

被鉴别的本体本身或者是代表本体的实体。

注：声称方拥有其代表本体从事鉴别交换时所必需的功能和私有数据。

[来源：GB/T 25069—2022,3.535]

3.4

验证方 verifier

要求鉴别其他实体身份的实体本身或其代表。

注：验证方包含了从事鉴别交换所必需的功能。

[来源：GB/T 25069—2022,3.708]

3.5

时间戳 time stamp;TS

对时间和其他待签名数据进行签名得到的,用于表明数据时间属性的数据。

[来源：GB/T 25069—2022,3.541]

3.6

可信第三方 trusted third party;TTP

在安全相关活动方面，被其他实体信任的安全机构或其代理。

[来源：GB/T 25069—2022,3.334]

4 符号

下列符号适用于本文件。

A,B 参与鉴别机制的实体的标签。

d_K 使用秘密密钥K的可鉴别解密过程。

e_K 使用秘密密钥K的可鉴别加密过程。

$e_K(X)$ 利用秘密密钥K对数据X使用可鉴别的加密算法进行加密的结果。

I_U 实体U的可区分标识符。

K 用于加密或解密的秘密密钥。

K_{UV} 由实体U和实体V共享的秘密密钥，只在可鉴别加密技术中使用。

N_U 由实体U产生的序号。

P 用以表示可信第三方的标识符。

R_U 由实体U产生的随机数。

SID^i_m 可唯一标识鉴别机制的字符串（m）以及机制中可鉴别加密实例的常量（数字i）。

TN_U 由实体U产生的时变参数，可以是时间戳T_U或序号N_U。

$Token_{UV}$ 从实体U向实体V发送的令牌。

T_U 由实体U产生的时间戳。

TVP_U 由实体U产生的时变参数，可以是时间戳T_U或序号N_U或随机数R_U。

X‖Y 数据项X和Y按照给定顺序级联的结果。当两个或多个数据项级联的结果在本文件的某个机制中被加密使用时，级联结果应该是编排的，以便可被唯一地解析为原来的构成项，即解析的时候不存在歧义。

注：这可以通过多种方式实现（具体取决于应用），例如(a)要求被级联的每个数据项的长度是固定且全程保持不变的，或(b)采用能确保唯一解码的方式对级联的序列进行编码，以确保正确解码，比如说采用GB/T 16263.1定义的非典型编码规则（Distinguished Encoding Rules，DER）。

5 总则

本文件规定的鉴别机制中，待鉴别的实体通过表明它知道某秘密密钥来证实其身份。这可由该实体用其秘密密钥加密特定数据达到，与其共享秘密密钥的任何实体都可以将加密后的数据解密。被解密的数据必须包含时变参数，时变参数可通过以下方式验证。

a) 如果时变参数是随机数，那么接收方应确保它与声称方发送的随机挑战是等同的，有关随机数的产生以及使用，参见 GM/T 0078。

b) 如果时变参数是时间戳，那么接收方应能够验证时间戳的有效性，有关时间戳的使用以及验证，参见 GB/T 15843.1—2017 的附录 B。

c) 如果时变参数是序号，那么接收方应能够将其与之前接收或存储的序号进行比较，以确保它不是之前的重放，有关序号的使用以及验证，参见 GB/T 15843.1—2017 的附录 B。

本文件中规定的机制采用诸如随机数、时间戳、序号等时变参数，来防止先前有效的鉴别信息被再次接受或被多次接受。

没有可信第三方参与时，采用时间戳或序号的方法，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信息；采用使用随机数的挑战-响应方法，对于单向鉴别需传递两次信息，而相互鉴别则需传递三次信息。有可信第三方参与时，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。

附录A定义了可用于标识本文件指定机制的对象标识符。附录B描述了文本字段使用的信息。附录C描述了本文件指定实体鉴别机制的主要特性。

6 要求

本文件所规定的鉴别机制应满足下列所有要求。

a) 向验证方证实其身份的声称方，在应用第 7 章的机制时，应和该验证方共享一个秘密密钥，在应用第 8 章的机制时，每个实体应和公共的可信第三方都分别共享一个秘密密钥。这些密钥应当在启动鉴别机制之前就被相关方获知（具体如何实现不在本文件的范围），关于共享密钥的管理，可参考 GB/T 17901.1 和 ISO/IEC 11770-2。

b) 如果涉及可信第三方，它应得到声称方与验证方的共同信任。

c) 声称方与验证方共享的秘密密钥，或实体与可信第三方共享的秘密密钥，应仅为这两方或双方都信任的其他方获知。若为双方都信任的其他方获知，则被信任的其他方不应误用密钥，即不应冒充双方之一来使用密钥。

注：在选择可鉴别的加密算法和确定密钥生存期时，应保证密钥在其生存期内就被推算出来在计算上是不可行的。此外，在选择密钥生存期时，还应防止已知明文和选择明文攻击。

d) 在机制中使用的令牌即使在已知旧令牌的情况下也不可被伪造，即在任何情况下旧令牌都不应被部分或全部重用来构造新令牌。对于秘密密钥 K 的任何取值，可鉴别加密函数 e_K 以及与它对应的可鉴别解密函数 d_K 应具有如下的属性：当解密过程 d_K 被应用到串 $e_K(X)$ 时，它应能够使得该串的接收方可以检测出数据是否被伪造或被篡改，即只有秘密密钥 K 的拥有者才能够通过解密过程 d_K 产生可被“接受”的串。

注：在实际应用中，可以通过很多方法来保证这一点。相比于其他方法，采用可鉴别加密技术，可以方便地同时提供机密性和完整性保护。本文件规定的鉴别机制即采用可鉴别加密技术，参见GB/T 36624。

e) 本文件中的机制要求使用时变参数，例如时间戳、序号或随机数。这些参数的特性，尤其是它们在秘密密钥的生命周期内极不可能重复的特性，对于这些机制的安全性是十分重要的。有关时变参数的更多信息，参见 GB/T 15843.1—2017 的附录 B。

f) 用来执行本文件所定义的任一鉴别机制的秘密密钥应与被用于其它用途的密钥区分开来。

g) 在一个鉴别机制中，如果存在多个被分别可鉴别加密的数据串，那么要确保这些密文数据串不能被互换使用。为了帮助实现这一要求，本文件中的机制在加密数据中包含常量 SID^{i}_{m}，接收方应验证鉴别加密数据中的常量 SID^{i}_{m} 是否符合预期。

注：本文件不明确要求常量的形式，按照需要，常量可被定义为包含下列元素：

——附录A定义的对象标识符，特别是标识了ISO标准和鉴别机制编号的标识符；

——在一个机制内唯一标识被鉴别加密数据串的常数，如果机制中仅包含一个签名数据串，则这个常数可以被略去。

h) 在第 8 章定义的机制中，K_{AP}（或 K_{BP}）密钥的持有者应以确定角色使用密钥，即要么作为 TTP（P），要么作为实体 A（或 B）。该密钥持有者不应使用相同的密钥，在某个鉴别协议执行实例中作为 TTP 参与的同时，又在该鉴别协议的另一个执行实例中作为实体 A 或 B 参与。

i) 根据可鉴别的加密算法的要求，应生成该可鉴别的加密算法的初始化向量（IV）。在多数情况下，这意味着在使用同一密钥多次执行可鉴别的加密算法的过程中，IV 应该是不同的。

7 不涉及在线可信第三方的机制

7.1 概述

这些鉴别机制中，实体A和B在开始具体运行鉴别机制之前应共享一个公共的秘密密钥K_{AB}，或者两个单向秘密密钥K_{AB}和K_{BA}。在后一种情况下，实体A总是使用单向密钥K_{AB}进行加密，而实体B总是使用其进行解密(反过来，对于密钥K_{BA}也是如此)。

以下机制中指定的所有文本字段在具体的鉴别应用中被赋予含义,有关这些应用的描述超出本文件范围。这些文本字段也可以是空的，它们的关系与内容取决于具体的应用。有关文本字段的使用见附录B。

7.2 单向鉴别

7.2.1 概述

单向鉴别是指使用该机制时两实体中只有一方被鉴别。

7.2.2 机制 UNI.TS——单次传递鉴别

在这种鉴别机制中，声称方A发起流程，并由验证方B进行鉴别。通过生成和检查时间戳或序号（见GB/T 15843.1—2017的附录B）来控制唯一性或时效性。

鉴别机制如图1所示。

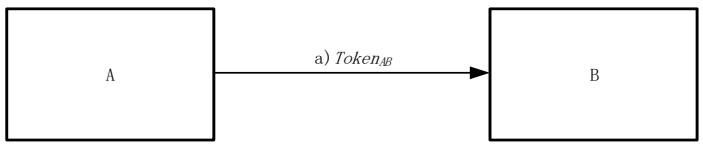

图1 机制 UNI.TS——单次传递鉴别

声称方A发送给验证方B的令牌（$Token_{AB}$）形式是：

$$Token_{AB} = Text_2 || e_{K_{AB}}(SID^1_{UNI.TS} || TN_A || I_B || Text_1)$$

此处声称方A或者用序号N_A，或者用时间戳T_A作为时变参数TN_A。具体选择哪一个取决于声称方与验证方的技术能力及环境。

在$Token_{AB}$中是否包含可区分标识符I_B是可选的。

注：在$Token_{AB}$中包含可区分标识符I_B是为防止敌手假冒实体B对实体A重用$Token_{AB}$。包含可区分标识符I_B之所以被作为可选项，是因为在不会出现这类攻击的环境中可将标识符省去。如果使用了单向密钥，该可区分标识符I_B也可以被省去。

下面是对机制UNI.TS——单次传递鉴别的描述：

a) A 产生并向 B 发送 $Token_{AB}$；

b) 一旦收到包含 $Token_{AB}$的消息，B 便通过解密和验证在此鉴别模式下的加密部分，以及检验 SID 来验证 $Token_{AB}$。然后 B 检验可区分标识符 I_B（如果有）以及时间戳或序号的正确性。

7.2.3 机制 UNI.CR——两次传递鉴别

这种鉴别机制中，验证方B启动此过程并对声称方A进行鉴别。唯一性或时效性是通过产生并检验随机数R_B（见GB/T 15843.1—2017中的附录B）来控制的。

鉴别机制如图2所示。

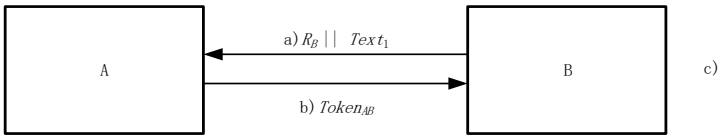

图2 机制 UNI.CR——两次传递鉴别

由声称方A发送给验证方B的令牌（$Token_{AB}$）形式是：

$$Token_{AB} = Text_3 || e_{K_{AB}}(SID^1_{UNI.CR} || R_B || I_B || Text_2)$$

在$Token_{AB}$中是否包含可区分标识符I_B是可选的。

注1：为了防止可能的选择明文攻击（即一种密码分析攻击，密码破译者知道一个或多个密文串对应的完整明文），实体 A 可以在 $Text_2$中包含一个随机数 R_A。

注2：在 $Token_{AB}$中包含可区分标识符 I_B是为了防止敌手假冒实体 B 对实体 A 重用 $Token_{AB}$。对可区分标识符 I_B的包含之所以是可选的，是因为在不可能发生此类攻击的环境中，可以将其省去。如果使用了单向密钥，可区分标识符 I_B也可以被省去。

下面是对机制UNI.CR——两次传递鉴别的描述：

a) B 产生一个随机数 R_B并向 A 发送，并可选地发送一个文本字段 $Text_1$给 A；

b) A 产生并向 B 发送 $Token_{AB}$；

c) 一旦收到包含 $Token_{AB}$的消息，B 便通过解密和验证在此鉴别模式下的加密部分以及检验 SID 来验证 $Token_{AB}$。然后 B 检验可区分标识符 I_B（如果有）的正确性以及在步骤 a)中发送给 A 的随机数 R_B是否与 $Token_{AB}$中所含的随机数相符。

7.3 相互鉴别

7.3.1 概述

相互鉴别是指两个通信实体运用该机制彼此进行鉴别。

7.3.2和7.3.3分别采用7.2.2和7.2.3中描述的两种机制，以实现相互鉴别。这两种情况都要求增加一次传送，从而增加了两个操作步骤。

7.3.2 机制 MUT.TS——两次传递鉴别

这种鉴别机制中，唯一性或时效性是通过产生并校验时间戳或序号（见GB/T 15843.1—2017的附录B）来控制的。鉴别机制如图3所示。

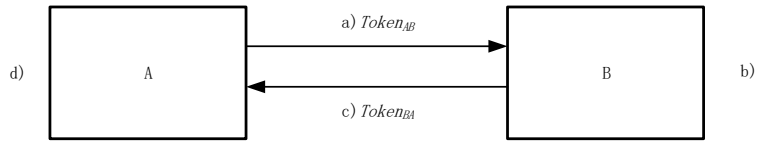

图3　机制 MUT.TS——两次传递鉴别

由A发送给B的令牌（$Token_{AB}$）形式与7.2.2规定的相同。

$Token_{AB} = Text_2||e_{K_{AB}}(SID^1_{MUT.TS}||TN_A||I_B||Text_1)$

由B发送给A的令牌（$Token_{BA}$）形式是：

$Token_{BA} = Text_4||e_{K_{AB}}(SID^2_{MUT.TS}||TN_A||TN_B||I_A||Text_3)$

在$Token_{AB}$中是否包含可区分标识符I_B,在$Token_{BA}$中是否包含可区分标识符I_A，是分别可选的。

注1：$Token_{AB}$中的可区分标识符 I_B是为防止敌手假冒实体 B 对实体 A 重用 $Token_{AB}$。同样的原因，$Token_{BA}$包含可区分标识符 I_A。可区分标识符的包含之所以作为可选项，是因为在不会出现这类攻击的环境中可以将其中之一或二者都省去。如果使用了单向密钥，可区分标示符 I_A和 I_B也可以被省去。

注2：如果 $Token_{BA}$中的 TN_A被省去，那么这种机制中两条消息之间除了时效性的隐含关系外没有任何绑定关系。该机制不再实现相互鉴别。

注3：如果 A 重用 TN_A，那么 $Text_1$就不能被可靠地验证。因此，A 在每个会话中都应使用各不相同的 TN_A。

这种机制中，选择使用时间戳还是序号取决于声称方与验证方的技术能力和环境。

下面是对机制MUT.TS——两次传递鉴别的描述：

a)　A 产生并向 B 发送 $Token_{AB}$;

b)　一旦收到包含 $Token_{AB}$ 的消息，B 便通过解密和验证在此鉴别模式下的加密部分以及检验 SID 来验证 $Token_{AB}$。然后 B 检验可区分标识符 I_B（如果有）以及时间戳或序号的正确性；

c)　B 产生并向 A 发送 $Token_{BA}$;

d)　一旦收到包含 $Token_{BA}$ 的消息，A 便通过解密和验证在此鉴别模式下的加密部分以及检验 SID 来验证 $Token_{BA}$。然后 A 检验可区分标识符 I_A（如果有）以及时间戳或序号的正确性。A 也同时验证收到的 TN_A与之前发送的 $Token_{AB}$中所含的时变参数是否相符。

如果使用了单向密钥，那么$Token_{BA}$中的密钥K_{AB}被密钥K_{BA}代替，并且在步骤d）中使用对应的密钥。

7.3.3　机制 MUT.CR——三次传递鉴别

这种鉴别机制中，唯一性或时效性是通过产生并校验随机数（见GB/T 15843.1—2017中的附录B）来控制的。

鉴别机制如图4所示。

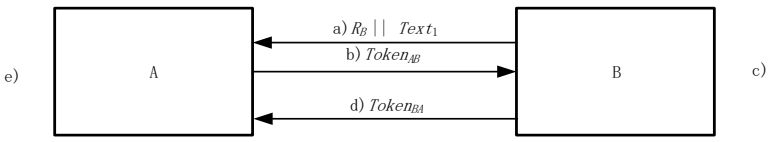

图4　机制 MUT.CR——三次传递鉴别

令牌形式如下：

$Token_{AB} = Text_3||e_{K_{AB}}(SID^1_{MUT.CR}||R_A||R_B||I_B||Text_2)$

$Token_{BA} = Text_5||e_{K_{AB}}(SID^2_{MUT.CR}||R_A||I_A||Text_4)$

$Token_{AB}$中是否包含可区分标识符I_B是可选的。

注：当$Token_{AB}$中包含可区分标识符I_B时，是为防止敌手假冒实体B对实体A重用$Token_{AB}$。可区分标识符I_B的包含之所以作为可选项，是因为在不会出现这类攻击的环境中可将其省去。如果使用了单向密钥，该可区分标识符I_B也可以被省去。$Token_{BA}$中包含I_A的情况相同。

下面是对机制MUT.CR——三次传递鉴别的描述：

a) B 产生一个随机数 R_B 并向 A 发送，并可选地发送一个文本字段 $Text_1$ 给 A；

b) A 产生一个随机数 R_A，然后产生 $Token_{AB}$ 并发送给 B；

c) 一旦收到包含 $Token_{AB}$ 的消息，B 便通过解密和验证在此鉴别模式下的加密部分以及检验 SID 来验证 $Token_{AB}$。然后 B 检验可区分标识符 I_B（如果有）的正确性以及步骤 a)中发给 A 的随机数 R_B 是否与 $Token_{AB}$ 中含的随机数相符；

d) B 产生并向 A 发送 $Token_{BA}$；

e) 一旦收到包含 $Token_{BA}$ 的消息，A 便通过解密和验证在此鉴别模式下的加密部分以及检验 SID 来验证 $Token_{BA}$。然后 A 检验在步骤 b)中发送给 B 的随机数 R_A 是否与 $Token_{BA}$ 中的随机数相符。

如果使用了单向密钥，那么$Token_{BA}$中的密钥K_{AB}被密钥K_{BA}代替，并且在步骤e)中使用对应的密钥。

8 涉及在线可信第三方的机制

8.1 概述

本章中所述的鉴别机制不是利用两个实体在鉴别过程前共享的秘密密钥，而是利用一个可信第三方（用P表示），实体A和B分别与它共享秘密密钥K_{AP}和K_{BP}。每个机制中，先由一个实体向可信第三方申请密钥K_{AB}，此后再分别采用7.3.2和7.3.3中描述的机制。

注：如果使用了单向密钥，那么自动满足第6章中的要求h）。但是，如果使用了双向密钥，这个要求可以通过机制本身之外的策略规则来约束。

按照下面的描述，如果只要求单向鉴别，则可省略每个机制中的某些传递。

以下机制中指定的所有文本字段在具体的鉴别应用中被赋予含义，有关这些应用的描述超出本文件范围。它们的关系和内容取决于具体应用。有关文本字段使用的信息参见附录B。

8.2 机制 TP.TS——四次传递鉴别

鉴别机制如图5所示。

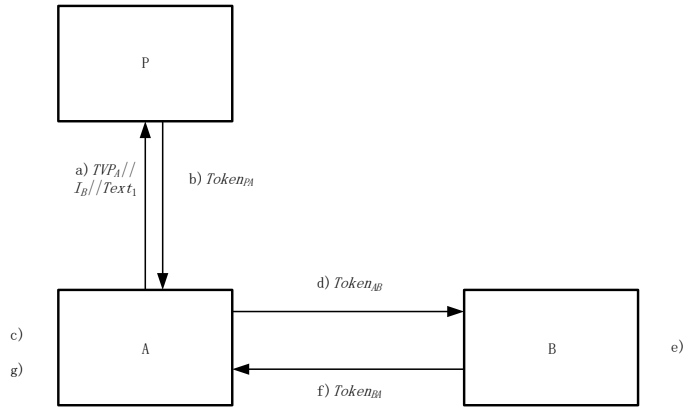

图5 机制 TP.TS——四次传递鉴别

由P发送给A的令牌（$Token_{PA}$）形式是：

$$Token_{PA} = Text_4||e_{K_{AP}}(SID^1_{TP.TS}||TVP_A||K_{AB}||I_B||Text_3)||e_{K_{BP}}(SID^2_{TP.TS}||TN_P||K_{AB}||I_A||Text_2)$$

由A发送给B的令牌（$Token_{AB}$）形式是：

$$Token_{AB} = Text_6||e_{K_{BP}}(SID^2_{TP.TS}||TN_P||K_{AB}||I_A||Text_2)||e_{K_{AB}}(SID^3_{TP.TS}||TN_A||Text_5)$$

由B发送给A的令牌（$Token_{BA}$）形式是：

$$Token_{BA} = Text_8||e_{K_{AB}}(SID^4_{TP.TS}||TN_B||Text_7)$$

在本机制中选择时间戳还是序号取决于相关实体的技术能力和环境。

在图5中步骤a）到步骤c）中的时变参数TVP_A的使用方法与通常的有所不同，它允许A将响应消息b）与请求消息a）联系起来。此处时变参数的重要特性是它的不可重复性，以限制先前用过的$Token_{PA}$被重用。

注：时变参数TVP_A可以是一个随机数。但是与本文件中某些机制所使用的随机数不同的是，该随机数对于第三方不必是不可预测的，不重复的计数器值同样适用于产生该随机数。

下面是对机制TP.TS——四次传递鉴别的描述：

a) A 产生并向可信第三方 P 发送一个时变参数 TVP_A、可区分标识符 I_B 以及可选地发送一个文本字段 $Text_1$；

b) 可信第三方 P 生成一个随机密钥 K_{AB}，同时产生并向 A 发送 $Token_{PA}$；

c) 一旦收到包含 $Token_{PA}$ 的消息，A 便通过解密和验证在此鉴别模式下使用 K_{AP} 加密的数据以及检验 SID 来验证 $Token_{PA}$。然后 A 检验可区分标识符 I_B 的正确性以及在步骤 a)中发送给 P 的时变参数是否与 $Token_{PA}$ 中的时变参数相符。此外，A 提取出秘密密钥 K_{AB}，然后再从 $Token_{PA}$ 中取出 $e_{K_{BP}}(SID^2_{TP.TS}||TN_P||K_{AB}||I_A||Text_2)$，并以此来构造$Token_{AB}$；

d) A 产生并向 B 发送 $Token_{AB}$；

e) 一旦收到包含 $Token_{AB}$ 的消息，B 便通过解密和验证在此鉴别模式下的加密部分以及检验 SID 来验证 $Token_{AB}$。然后 B 检验可区分标识符 I_A 以及时间戳或序号的正确性。此外，B 提取出秘密密钥 K_{AB}；

f) B 产生并向 A 发送 $Token_{BA}$；

g) 一旦收到包含 $Token_{BA}$ 的消息，A 便通过解密和验证在此鉴别模式下的加密部分以及检验 SID 来验证 $Token_{BA}$。然后检验时间戳或序号的正确性。

如果只要求B对A的单向鉴别，步骤f)和g)可省去。

8.3 机制 TP.CR——五次传递鉴别

在这种相互鉴别机制中，唯一性或时效性是用随机数（见GB/T 15843.1—2017的附录B）来控制的。鉴别机制如图6所示。

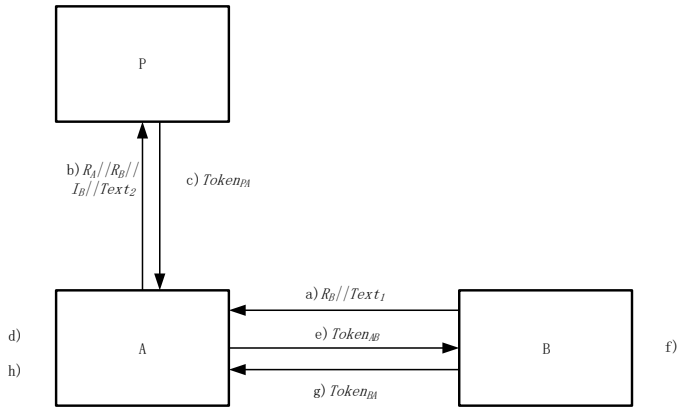

图6 机制 TP.CR——五次传递鉴别

由P发送给A的令牌（$Token_{PA}$）形式是：

$$Token_{PA} = Text_5||e_{K_{AP}}(SID^1_{TP.CR}||R_A||K_{AB}||I_B||Text_4)||e_{K_{BP}}(SID^2_{TP.CR}||R_B||K_{AB}||I_A||Text_3)$$

由A发送给B的令牌（$Token_{AB}$）形式是：

$$Token_{AB} = Text_7||e_{K_{BP}}(SID^2_{TP.CR}||R_B||K_{AB}||I_A||Text_3)||e_{K_{AB}}(SID^3_{TP.CR}||R'_A||R_B||Text_6)$$

由B发送给A的令牌（$Token_{BA}$）形式是：

$$Token_{BA} = Text_9||e_{K_{AB}}(SID^4_{TP.CR}||R'_A||Text_8)$$

下面是对机制TP.CR——五次传递鉴别的描述：

a) B产生并向A发送一个随机数R_B，可选地发送一个文本字段$Text_1$；

b) A产生随机数R_A，并向可信第三方P发送R_A、随机数R_B、可区分标识符I_B以及可任选地发送一个文本字段$Text_2$；

c) 可信第三方P生成一个随机密钥K_{AB}，同时产生并向A发送$Token_{PA}$；

d) 一旦收到包含$Token_{PA}$的消息，A便通过解密和验证在此鉴别模式下使用K_{AP}加密的数据以及检验SID来验证$Token_{PA}$。然后A检验可区分标识符I_B的正确性以及在步骤b)中发给P的随机数R_A是否与$Token_{PA}$中的随机数相符。此外，A提取出秘密密钥K_{AB},然后再从$Token_{PA}$中取出$e_{K_{BP}}(SID^2_{TP.CR}||R_B||K_{AB}||I_A||Text_3)$，以此来构造$Token_{AB}$；

e) A产生第二个随机数R'_A，然后产生并向B发送$Token_{AB}$；

f) 一旦收到包含$Token_{AB}$的消息，B便通过解密和验证在此鉴别模式下的加密部分以及检验SID来验证$Token_{AB}$。然后B检验可区分标识符I_A的正确性以及在步骤a)中发给A的随机数R_B是否与$Token_{AB}$中的该随机数的两个副本相符。此外，B还提取出秘密密钥K_{AB}；

g) B产生并向A发送$Token_{BA}$；

h) 一旦收到包含$Token_{BA}$的消息，A便通过解密和验证在此鉴别模式下的加密部分以及检验SID来验证$Token_{BA}$。然后A检验在步骤e)中发送给B的随机数R'_A是否与$Token_{BA}$中包含的那个随机数相符。

如果只要求B对A的单向鉴别，步骤g)和h)可以被省去。

附 录 A
（规范性）
对象标识符

附录A定义了本文件指定机制的对象标识符。

A.1 形式化定义

```
EntityAuthenticationMechanisms-2 {
    iso(1) standard(0) e-auth-mechanisms(9798) part2(2)
       asn1-module(0) object-identifiers(0) }
    DEFINITIONS EXPLICIT TAGS ::= BEGIN

-- EXPORTS All; --
-- IMPORTS None; --

OID ::= OBJECT IDENTIFIER -- alias
-- Synonyms --
is9798-2 OID ::= { iso(1) standard(0) e-auth-mechanisms(9798) part2(2) }
mechanism OID ::= { is9798-2 mechanisms-2019 (2) }

-- 不涉及可信第三方的单向或相互实体鉴别机制 --
nottp-mechanism OID ::= { mechanism nottp(1) }
nottp-uni-mechanism OID ::= { nottp-mechanism uni(1) }
nottp-mut-mechanism OID ::= { nottp-mechanism mut(2) }
uni-ts OID ::= { nottp-uni- mechanism 1 }
uni-cr OID ::= { nottp-uni- mechanism 2 }
mut-ts OID ::= { nottp-mut- mechanism 1 }
mut-cr OID ::= { nottp-mut- mechanism 2 }

-- 涉及可信第三方的相互实体鉴别机制 -
ttp- mechanism OID ::= { mechanism ttp(2) }
ttp-mut-1 OID ::= { ttp- mechanism 1 }
ttp-mut-2 OID ::= { ttp- mechanism 2 }

END -- EntityAuthenticationMechanisms-2 --
```

A.2 对象标识符的后续使用

本文件中所有的实体鉴别机制都使用可鉴别加密技术。因此，在实体鉴别机制的对象标识符之后，可能会跟有一个对象标识符来指定所使用的加密技术，例如在GB/T 36624中所定义的各个机制的对象标

识符以及所有相关参数，例如在GB/T 36624中进一步指明的分组密码加密机制标识符、分组密码工作模式和/或消息鉴别码（Message Authentication Code，MAC）算法。

附 录 B
（资料性）
文本字段的使用

本文件的第7章和第8章规定的令牌包含了文本字段。在给定传递中不同文本字段的实际使用及各文本字段间的关系取决于具体应用。以下给出一个实例，也可以参考GB/T 15843.1-2017的附录A。

机密性或数据源鉴别所需的信息应被放在该令牌的被加密部分。

加密的文本字段可以用来表明该令牌仅在用于实体鉴别时有效。如果担心一个实体可能会出于恶意选择一个数让另一个实体加密，那么另一个实体可以在文本字段中引入随机数。

文本字段还可以用于向验证者提供信息，表明声称方所声明的(未经鉴别的)身份。可以要求此类信息，以允许验证者确定将使用哪个密钥来对声称方进行身份鉴别。

附 录 C
（资料性）
实体鉴别机制的特性

表C.1总结了本文件所描述的实体鉴别机制的主要特性。括号中显示的是可选项，例如，机制TP.TS有一个可选的三次传递单向鉴别版本。

表C.1 机制的特性

机制	UNI.TS	UNT.CR	MUT.TS	MUT.CR	TP.TS	TP.CR
传递的次数	1	2	2	3	4（或3）	5（或4）
单向/相互鉴别	单向	单向	相互	相互	相互（单向）	相互（单向）
保证时效性的变量(注1)	TN_A	R_B	TN_A和TN_B	R_A和R_B	TVP_A, TN_B和TN_P	R_A和R_B
发起鉴别机制的实体	A	B	A	B	A	B
声称方是否获知成功信息（注2）	否	否	仅A获知	仅A获知	仅A获知	仅A获知

注1：对于使用随机数来保证时效性的机制 UNI.CR、MUT.CR 和 TP.CR，两实体间不必维持同步时钟或序号。

注2：在本文件所描述的鉴别机制中，声称方以加密令牌的形式发送身份证明。某些情况下，对方实体并不返回响应以表明身份证明被成功地接受。表 C.1 中的最后一行表明了协议内在的保证成功鉴别的信息的位置。在其余的情况下，如果声称方需要，则系统必须向其提供成功信息。

参 考 文 献

[1] GB/T 15852.1 信息技术 安全技术 消息鉴别码 第1部分:采用分组密码的机制

[2] GB/T 15843.5 信息技术 安全技术 实体鉴别 第5部分：使用零知识技术的机制

[3] GB/T 16263.1 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

[4] GB/T 17901.1 信息技术 安全技术 密钥管理 第1部分：框架

[5] GB/T 17964 信息安全技术 分组密码算法的工作模式

[6] GB/T 32907 信息安全技术 SM4分组密码算法

[7] GM/T 0078 密码随机数生成模块设计指南

[8] ISO/IEC 8824(all parts),Information technology—Abstract Syntax Notation One(ASN.1)

[9] ISO/IEC 11770-2,IT Security techniques—Key management—Part 2: Mechanisms using symmetric techniques

[10] ISO/IEC 18031,Information technology—Security techniques—Random bit generation

[11] BASIN D.,CREMERS C.,MEIER S.‘Provably repairing the ISO/IEC 9798 standard for entity authentication’. In: P. Degano, J. D. Guttman (eds.), Principles of Security and Trust - First International Conference, POST 2012, Tallinn, Estonia, March 24 – April 1, 2012, Proceedings. Springer LNCS 7215, pp.129-148, 2012