ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 15843.2—2024
代替 GB/T 15843.2—2017

网络安全技术　实体鉴别
第2部分：采用鉴别式加密的机制

Cybersecurity technology—Entity authentication—Part 2：Mechanisms using authenticated encryption

（ISO/IEC 9798-2：2019，IT Security techniques—Entity authentication—Part 2：Mechanisms using authenticated encryption，MOD）

2024-09-29 发布　　2025-04-01 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》的规定起草。

本文件是GB/T 15843的第2部分。GB/T 15843已经发布了以下部分：

——信息技术　安全技术　实体鉴别　第1部分：总则；

——网络安全技术　实体鉴别　第2部分：采用鉴别式加密的机制；

——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；

——网络安全技术　实体鉴别　第4部分：采用密码校验函数的机制；

——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；

——信息技术　安全技术　实体鉴别　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，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了标准适用范围和适用对象的描述，删除了“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）；

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

c) 增加了符号“SID_m^i”（见第4章、第6章、第7章、第8章及附录A），增加了缩略语“DER”“MAC”（见4.2）；

d) 增加了“通则”，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）；

e) 将“要求”中“对称加密”更改为“鉴别式加密”并修改了表述（见第6章，2017年版的第5章）；

f) 增加了初始化向量的相关要求（见第6章）；

g) 将“可信第三方”更改为“在线可信第三方”并修改了表述（见第7章及第8章，2017年版的第6章及第7章）；

h) 将各类机制的标识符，由数字更改为英文缩写（见第4章、第7章、第8章、附录A，2017年版的第6章、第7章、附录A）；

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

本文件修改采用ISO/IEC 9798-2:2019《信息安全技术　实体鉴别　第2部分：采用鉴别式加密的机制》。

本文件与ISO/IEC 9798-2:2019相比做了下述结构调整：

——4.1对应ISO/IEC 9798-2:2019的第4章，并增加了4.2；

——增加了附录D。

本文件与ISO/IEC 9798-2:2019的技术差异及其原因如下：

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

- 用规范性引用的GB/T 15843.1—2017替换了ISO/IEC 9798-1（见第3章），用规范性引用

的 GB/T 36624 替换了 ISO/IEC 19772(见第 3 章及第 6 章);

- 用规范性引用的 GB/T 16262(所有部分)替换了 ISO/IEC 8824(所有部分)(见附录 A);
- 增加了规范性引用 GB/T 25069—2022(见第 3 章);

——为保证与国家标准的协调一致,在“术语和定义”一章引导语增加了引用文件 GB/T 25069(见第 3 章);

——为保证与国家标准的协调一致,增加了“验证方”术语及定义(见第 3 章),删除了 ISO/IEC 9798-2:2019 的“密文”术语及定义;

——为保证文件的可读性,修改了符号“A,B”“I_U”“K_{UV}”“N_U”“R_U”“TN_U”“$Token_{UV}$”“T_U”“TVP_U”,增加了符号“IV”“R'_X”“$Text_n$”“$MUT.CR$”“$MUT.TS$”“$TTP.CR$”“$TTP.TS$”“$UNI.CR$”“$UNI.TS$”“‖”(见 4.1);

——为保持文本前后内容一致,保证文本的可读性,修改涉及在线可信第三方的机制标识符,将“$TP.TS$”更改为“$TTP.TS$”,将“$TP.CR$”更改为“$TTP.CR$”(见 4.1、第 8 章)。

本文件做了下列编辑性改动:

——根据国内实际情况,修改文件名称为“网络安全技术　实体鉴别　第 2 部分:采用鉴别式加密的机制”;

——删除了 ISO/IEC 9798-2:2019 第 1 章中对于附录 A 的说明,调整至第 5 章(见第 5 章);

——第 5 章增加了资料性引用的 GM/T 0078、GM/T 0103 及 GM/T 0105(见第 5 章);

——第 6 章用资料性引用的 GB/T 17901.1 替换了 ISO/IEC 11770-1(见第 6 章);

——增加了资料性附录“机制 $MUT.CR$——三次传递鉴别参考示例”(见附录 D)。

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专利的责任。

本文件由全国网络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、中国电子技术标准化研究院、中国科学院大学、国家密码管理局、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、陕西省信息化工程研究院、云南电网有限责任公司信息中心、北京时代亿信科技股份有限公司、郑州信大捷安信息技术股份有限公司、中国科学院软件研究所、公安部第三研究所、兴唐通信科技有限公司、北京信安世纪科技股份有限公司、长扬科技(北京)股份有限公司、北京时代新威信息技术有限公司、联通在线信息科技有限公司、中国科学院信息工程研究所、北京国脉信安科技有限公司、华为技术有限公司、鼎铉商用密码测评技术(深圳)有限公司、启明星辰信息技术集团股份有限公司。

本文件主要起草人:刘中、夏鲁宁、李彦峰、荆继武、王鹏、田敏求、林阳荟晨、王琼霄、郑亚杰、李向锋、王跃武、高五星、朱鹏飞、郑强、闫斌、赵晓荣、肖鹏、刘伟丰、刘为华、张立武、杨元原、蔡子凡、张宇、赵华、朱威儒、傅大鹏、颜雪薇、田学娟、郭丽芳、魏东、张振红、张严、程福兴、贾世杰、马原、袁峰、曾光、陈磊、许雪姣、李鑫、王新杰、梁斌、封维端、肖飞、陈萧宇。

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 旨在规范实体鉴别机制中不同种类的实体鉴别协议，拟由 6 个部分组成。

——第 1 部分：总则。目的在于规范实体鉴别机制中的鉴别模型和一般性约束要求。

——第 2 部分：采用鉴别式加密的机制。目的在于规范六种采用鉴别式加密实现实体鉴别的机制及相关要求。

——第 3 部分：采用数字签名技术的机制。目的在于规范十种基于数字签名技术的实体鉴别机制及相关要求。

——第 4 部分：采用密码校验函数的机制。目的在于规范四种采用密码校验函数的实体鉴别机制及相关要求。

——第 5 部分：使用零知识技术的机制。目的在于规范三种使用零知识技术的实体鉴别机制及相关要求。

——第 6 部分：采用人工数据传递的机制。目的在于规范八种在设备之间基于人工数据传递进行实体鉴别的机制及相关要求。

网络安全技术　实体鉴别
第2部分：采用鉴别式加密的机制

1　范围

本文件规定了两类（共六种）采用遵循GB/T 36624的鉴别式加密实现实体鉴别的机制。第一类不引入在线可信第三方，包含两种单向鉴别机制和两种相互鉴别机制。第二类引入一个在线可信第三方，包含两种单向或相互的实体鉴别机制。

本文件适用于指导基于鉴别式加密实现的实体鉴别系统、产品或服务的设计、开发和测试等。

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 16262（所有部分）　信息技术　抽象语法记法一（ASN.1）[ISO/IEC 8824（所有部分）]

注：GB/T 16262.1—2006　信息技术　抽象语法记法一（ASN.1）第1部分：基本记法规范（ISO/IEC 8824-1：2002，IDT）；

GB/T 16262.2—2006　信息技术　抽象语法记法一（ASN.1）　第2部分：信息客体规范（ISO/IEC 8824-2：2002，IDT）；

GB/T 16262.3—2006　信息技术　抽象语法记法一（ASN.1）　第3部分：约束规范（ISO/IEC 8824-3：2002，IDT）；

GB/T 16262.4—2006　信息技术　抽象语法记法一（ASN.1）　第4部分：ASN.1规范的参数化（ISO/IEC 8824-4：2002，IDT）。

GB/T 25069—2022　信息安全技术　术语

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

3　术语和定义

GB/T 15843.1—2017、GB/T 25069—2022、GB/T 36624界定的以及下列术语和定义适用于本文件。

3.1

鉴别式加密　authenticated encryption

可逆的数据转换，这种数据转换利用密码算法产生数据的对应密文，未经授权实体无法在不被发现的情况下对其修改，同时提供了数据机密性、数据完整性与数据源鉴别。

注：本文件所定义的“鉴别式加密”，等同于GB/T 36624所定义的“可鉴别的加密”。

[来源：GB/T 25069—2022，3.298，有修改]

3.2

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]

3.3

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]

3.4

时间戳　time stamp

一种时变参数，代表公共时间基准下的某一个时间点。

注：见 GB/T 15843.1—2017 的附录 B。

[来源：GB/T 15843.1—2017，3.35]

3.5

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　符号和缩略语

4.1　符号

下列符号适用于本文件。

A：　参与鉴别机制的实体 A 的标签。当涉及多个实体时，也可用 B、C、D 等任何一个大写字母表示不同的实体。

d_K：　使用秘密密钥 K 的鉴别式解密过程。

e_K：　使用秘密密钥 K 的鉴别式加密过程。

$e_K(X)$：　利用秘密密钥 K 对数据 X 使用鉴别式加密进行加密的结果。

I_X：　实体 X 的可区分标识符，X 可为 A、B、C 等任何实体。

IV：　初始化向量，即在密码变换中，为增加安全性或使密码设备同步而引入的用于数据变换的起始数据。

K：　用于加密或解密的秘密密钥。

K_{XY}：　由实体 X 和实体 Y 共享的秘密密钥，只在鉴别式加密中使用。当作为单向秘密密钥时，实体 X 只用其进行加密，实体 Y 只用其进行解密。X、Y 可为 A、B、C 等任何实体，X、Y 不能为同一实体。

$MUT.CR$：　本文件中相互鉴别模式下三次传递鉴别机制的标识符。

$MUT.TS$：　本文件中相互鉴别模式下两次传递鉴别机制的标识符。

N_X：　由实体 X 产生的序号，X 可为 A、B、C 等任何实体。

P：　用以表示可信第三方的标识符。

R_X：　由实体 X 产生的随机数，X 可为 A、B、C 等任何实体。

R'_X：　由实体 X 在同一次鉴别中产生的第二个随机数，X 可为 A、B、C 等任何实体。

SID_m^i：　可唯一标识鉴别机制 m 中的鉴别式加密实例 i 的常量。在本文件中，m 表示本文

件规定的各种机制的标识符，i 为自然数，用以区分同一次实体鉴别中的加密实例。

T_X： 由实体 X 产生的时间戳，X 可为 A、B、C 等任何实体。

$Text_n$： 用以表示文本字段的标识符，本文件中用数字 n 区分不同的文本字段。

TN_X： 由实体 X 产生的时变参数，可为时间戳 T_X 或序号 N_X，X 可为 A、B、C 等任何实体。

$Token_{XY}$： 从实体 X 向实体 Y 发送的令牌，X、Y 可为 A、B、C 等任何实体，X、Y 不能为同一实体。

$TTP.CR$： 本文件中涉及在线可信第三方的鉴别模式下五次传递鉴别机制的标识符。

$TTP.TS$： 本文件中涉及在线可信第三方的鉴别模式下四次传递鉴别机制的标识符。

TVP_X： 由实体 X 产生的时变参数，可为时间戳 T_X 或序号 N_X 或随机数 R_X，X 可为 A、B、C 等任何实体。

$UNI.CR$： 本文件中单向鉴别模式下单次传递鉴别机制的标识符。

$UNI.TS$： 本文件中单向鉴别模式下两次传递鉴别机制的标识符。

$\|$： 数据项的级联。

$X \| Y$： 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：能通过多种方式实现（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，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，比如采用 GB/T 16263.1 定义的 DER（Distinguished Encoding Rules，ASN.1 的非典型编码规则）。

4.2 缩略语

下列缩略语适用于本文件。

DER：ASN.1 的非典型编码规则（Distinguished Encoding Rules）

MAC：消息鉴别码（Message Authentication Code）

5 通则

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实现，与其共享秘密密钥的任何实体都能将加密后的数据解密。被解密的数据应包含时变参数，时变参数能通过以下方式验证。

a） 如果时变参数是随机数，那么验证方应确保它与声称方发送的随机挑战是等同的，有关随机数的产生可参考 GM/T 0078、GM/T 0103、GM/T 0105 等。

b） 如果时变参数是时间戳，那么验证方宜能验证时间戳的有效性，有关时间戳的使用以及验证见 GB/T 15843.1—2017 的附录 B。

c） 如果时变参数是序号，那么验证方应能将其与之前接收或保存的序号进行比较，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 定义了应被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。附录D给出了机制*MUT.CR*——三次传递鉴别的参考示例。

6 要求

本文件所规定的鉴别机制满足下列所有要求。若其中任何一个不满足，则鉴别过程会面临潜在攻击或不能成功完成。

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，每个实体应和在线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，见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共同信任的其他方获知。若为双方共同信任的其他方获知，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1：在选择鉴别式加密和确定密钥生存期时，需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，还需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应被伪造，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。对于秘密密钥的任何取值，鉴别式加密过程e_K以及与它对应的鉴别式解密过程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，它应能使得该串的验证方可检测出数据是否被伪造或被篡改，即只有秘密密钥K的拥有者才能通过解密过程d_K产生可被“接受”的串。

注2：在实际应用中，可通过很多方法来保证这一点。相比于其他方法，采用鉴别式加密，可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鉴别式加密，遵循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。有关时变参数的更多信息，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不应被用于其他用途。

g) 在一个鉴别机制中，如果分别存在多个已被鉴别式加密的数据串，那么要确保这些密文数据串不应被互换使用。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_m^i，验证方应验证鉴别式加密数据中的常量SID_m^i是否符合预期。

注3：本文件不明确要求常量的形式，按照需要，常量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式加密数据串的常数，如果机制中仅包含一个被鉴别式加密的数据串，则这个常数被略去。

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)。即不应有实体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参与协议，并且该实体在两个实例中使用了相同的密钥。

i) 根据鉴别式加密的要求，应生成初始化向量IV。一般情况下，在使用同一密钥多次执行加密的过程中，IV宜是不同的。

7 不涉及在线可信第三方的机制

7.1 通则

这些鉴别机制中，实体 A 和 B 在开始具体执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。这些文本字段也可为空，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。通过生成和检查序号或时间戳来控制唯一性或时效性。

鉴别机制见图 1。

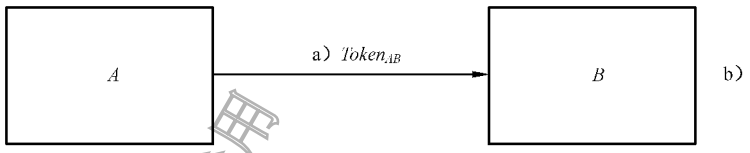

图 1 机制 *UNI.TS*——单次传递鉴别

声称方 A 发送给验证方 B 的令牌$Token_{AB}$形式是：

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

此处声称方 A 用序号N_A，或者时间戳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能将标识符省去。如果使用了单向秘密密钥，该可区分标识符I_B也能被省去。

下面是对机制 $UNI.TS$——单次传递鉴别的过程描述。

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^{i}_{m}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

在这种鉴别机制中，验证方 B 发起流程，并对声称方 A 进行鉴别。通过生成和检查随机数R_B来控制唯一性或时效性。

鉴别机制见图 2。

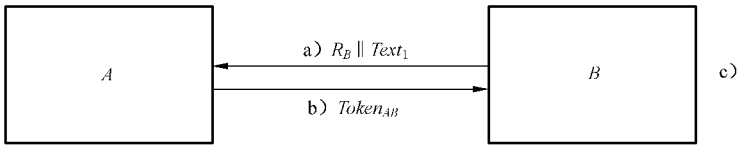

图 2　机制 *UNI.CR*——两次传递鉴别

由声称方 A 发送给验证方 B 的令牌$Token_{AB}$形式是：

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

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 能在$Text_2$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能将其省去。如果使用了单向秘密密钥，可区分标识符I_B也能被省去。

下面是对机制 $UNI.CR$——两次传递鉴别的过程描述。

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^i_m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。

7.3.2　机制 *MUT.TS*——两次传递鉴别

在这种鉴别机制中，通过生成和检查序号或时间戳来控制唯一性或时效性。

鉴别机制见图 3。

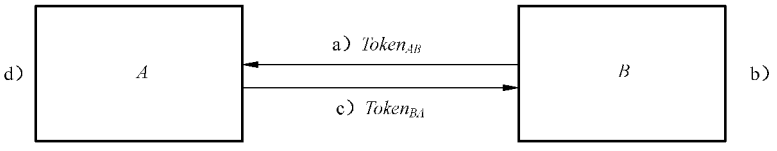

图 3　机制 *MUT.TS*——两次传递鉴别

由 A 发送给 B 的令牌$Token_{AB}$形式与 7.2.2 规定的相同。

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

由 B 发送给 A 的令牌$Token_{BA}$形式是：

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

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能将其中之一

或二者都省去。如果使用了单向秘密密钥，可区分标示符I_A和I_B也能被省去。

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 在不同会话中使用同一个TN_A是存在风险的。

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 $MUT.TS$——两次传递鉴别的过程描述。

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_m^i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。以上检查及验证均通过，则执行下一步。

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_m^i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

在这种鉴别机制中，通过生成和检查随机数来控制唯一性或时效性。

鉴别机制见图 4。

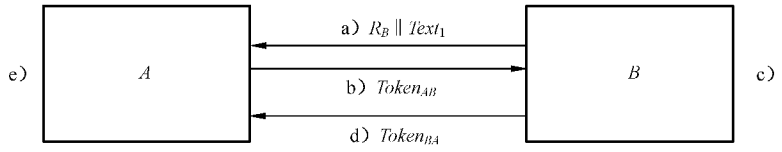

图 4　机制 *MUT.CR*——三次传递鉴别

令牌形式如下：

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

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

$Token_{AB}$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能将其省去。如果使用了单向密钥，该可区分标识符I_B也能被省去。$Token_{BA}$中包含I_A的情况相同。

下面是对机制 $MUT.CR$——三次传递鉴别的过程描述。

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_m^i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。以上检查及验证均通过，则执行下一步。

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_m^i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是利用一个可信第三方(用 P 表示)实现，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：如果使用了单向秘密密钥，那么自动满足第 6 章中的要求 h)；如果使用了双向秘密密钥，这个要求能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均有实际含义，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见附录 B。

8.2 机制 *TTP.TS*——四次传递鉴别

鉴别机制见图 5。

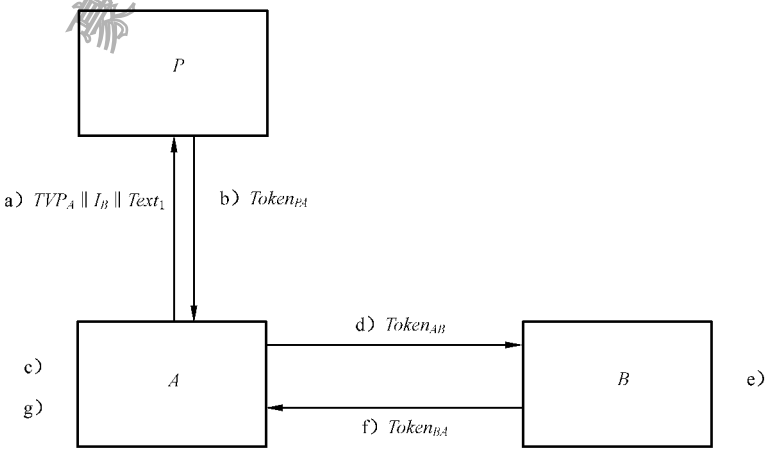

图 5 机制 *TTP.TS*——四次传递鉴别

由 P 发送给 A 的令牌$Token_{PA}$形式是：

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

由 A 发送给 B 的令牌$Token_{AB}$形式是：

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

由 B 发送给 A 的令牌$Token_{BA}$形式是：

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

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)～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可为一个随机数。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 $TTP.TS$——四次传递鉴别的过程描述。

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_m^i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。以上检查及验证均通过后，则 A 得到秘密密钥K_{AB}，然后再从$Token_{PA}$中取出$e_{K_{BP}}(SID_{TTP.TS}^2 \parallel TN_P \parallel K_{AB} \parallel I_A \parallel Text_2)$，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_m^i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}。以上检查及验证均通过后，则执行下一步。

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_m^i来验证$Token_{BA}$。然后检验时间戳或序号的正确性。

如果只要求 A 被 B 单向鉴别，步骤 f)和步骤 g)可省去。

8.3 机制 *TTP.CR*——五次传递鉴别

在这种相互鉴别机制中，通过随机数来控制唯一性或时效性。

鉴别机制见图 6。

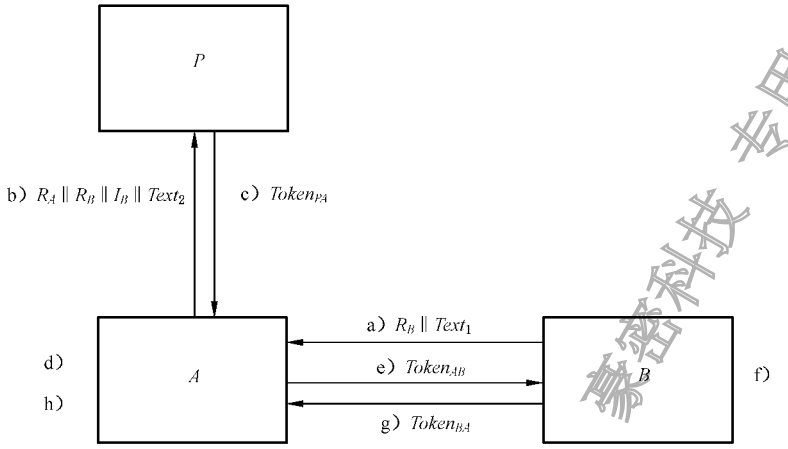

图 6 机制 *TTP.CR*——五次传递鉴别

由 P 发送给 A 的令牌$Token_{PA}$形式是：

$$Token_{PA} = Text_5 \parallel e_{K_{AP}}(SID_{TTP.CR}^1 \parallel R_A \parallel K_{AB} \parallel I_B \parallel Text_4) \parallel e_{K_{BP}}(SID_{TTP.CR}^2 \parallel R_B \parallel K_{AB} \parallel I_A \parallel Text_3)$$

由 A 发送给 B 的令牌$Token_{AB}$形式是：

$$Token_{AB} = Text_7 \parallel e_{K_{BP}}(SID_{TTP.CR}^2 \parallel R_B \parallel K_{AB} \parallel I_A \parallel Text_3) \parallel e_{K_{AB}}(SID_{TTP.CR}^3 \parallel R'_A \parallel R_B \parallel Text_6)$$

由 B 发送给 A 的令牌$Token_{BA}$形式是：

$$Token_{BA} = Text_9 \parallel e_{K_{AB}}(SID_{TTP.CR}^4 \parallel R'_A \parallel Text_8)$$

下面是对机制 $TTP.CR$——五次传递鉴别的过程描述。

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_m^i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。以上检查及验证均通过后，则 A 得到秘密密钥K_{AB}，然后再从 $Token_{PA}$ 中取出e_{KBP}（$SID_{TTP,CR}^2 \parallel R_B \parallel K_{AB} \parallel I_A \parallel Text_3$），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_m^i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。以上检查及验证均通过后，则 B 得到秘密密钥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_m^i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 A 被 B 单向鉴别，步骤 g)和步骤 h)可被省去。

附 录 A
（规范性）
对象标识符

A.1 形式化定义

本文件所规定机制的对象标识符定义如下，采用 GB/T 16262（所有部分）定义的抽象语法记法（ASN.1）来表示。

```
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 对象标识符的使用

本文件中所有的实体鉴别机制都使用鉴别式加密。因此，在实体鉴别机制的对象标识符之后，可能会跟有另一个对象标识符来指定所使用的加密技术，例如在 GB/T 36624 中规定的各个机制的对象标识符以及分组密码加密机制标识符、分组密码工作模式和/或 MAC 算法等所有相关参数。

附 录 B
（资料性）
文本字段的使用

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。例如：

机密性或数据源鉴别所需的信息放在该令牌的被加密的文本字段中。

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

文本字段还能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。能要求此类信息，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。

关于文本字段的使用，见 GB/T 15843.1—2017 的附录 A。

附 录 C
（资料性）
实体鉴别机制的主要特性

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 *TTP.TS* 有一个可选的三次传递单向鉴别版本。

表 C.1 机制的主要特性

机制特性	*UNI.TS*	*UNI.CR*	*MUT.TS*	*MUT.CR*	*TTP.TS*	*TTP.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 *TTP.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，则系统要求向其提供成功信息。

附 录 D
（资料性）
机制 *MUT.CR*——三次传递鉴别参考示例

D.1 概述

本附录以机制 *MUT.CR*——三次传递鉴别为例给出示例，作为实现本文件所规定机制的参考。

以下定义的参数及有关约定，仅适用于本示例。在不同的具体应用中，参数取值及约定按具体需求定义。

D.2 机制 *MUT.CR*——三次传递鉴别参考示例

D.2.1 前置参数定义

在机制 *MUT.CR*——三次传递鉴别机制中，实体 A 和实体 B 在鉴别前，需约定相关参数类型及生成方式。

本示例中验证双方需要的预置参数如表 D.1 所示。

a) IV 表示当密钥为K_{AB}时的初始向量。

b) 根据第 6 章 g)的要求，SID 的形式根据实际需要进行定义，本示例采用机制 *MUT.CR*，根据 7.3.3，此机制需定义$SID^1_{MUT.CR}$、$SID^2_{MUT.CR}$，分别表示由 A 和 B 产生的 SID。根据附录 A，*MUT.CR* 的 OID 为 1.0.9798.2.2.1.2.2，十六进制表示为{28 cc 46 02 02 01 02 02}，此部分是对 *MUT.CR* 的标识，即实体 A 与实体 B 的此部分相同。在此基础上，第 9 个字节(从左至右)用来区分 A 和 B 的 SID，如本示例中 0x01 表示 A 的 SID，0x02 表示 B 的 SID。最后 7 个字节用来表示第几次实体鉴别，如本示例中，A 和 B 的初始 SID 的最后一个字节均为“0x01”，表示此为 *MUT.CR* 机制的第一次实体鉴别，当双方完成一次鉴别之后，各自的 SID 加一，之后以此类推。验证方通过验证前 8 字节是否相同确定是否为约定的鉴别机制，通过第 9 个字节(从左至右)验证本次实体鉴别中的加密实例，通过验证后 7 个字节是否加一验证是否为新一次的实体鉴别。

c) I_A、I_B作为实体 A 与实体 B 的可区分标识符，需提前商定，并各自存储在本地。

d) 类型定义采用 C 语言。

表 D.1 预置参数定义

参数名	类型定义	预置值(十六进制)
K_{AB}	unsigned char [16]	{55 22 76 65 72 69 66 79 20 6d 75 74 5f 63 72 3b}
IV	unsigned char [16]	{31 32 33 34 35 36 37 38 61 62 63 64 65 66 67 68}
$SID^1_{MUT.CR}$	char[16]	{28 cc 46 02 02 01 02 02 01 00 00 00 00 00 00 01}
$SID^2_{MUT.CR}$	char[16]	{28 cc 46 02 02 01 02 02 02 00 00 00 00 00 00 01}
R_A	unsigned char [16]	{69 61 36 64 37 39 36 39 36 32 23 73 23 63 13 66}
R_B	unsigned char [16]	{07 00 0E 0F 0A 09 00 0F 00 00 00 00 00 00 00 66}
I_A	char[8]	{12 12 12 12 00 00 00 01}
I_B	char[8]	{21 21 21 21 00 00 00 01}

表 D.1 预置参数定义（续）

参数名	类型定义	预置值(十六进制)
$Text_1$	char[8]	{A1 00 00 00 00 00 00 66}
$Text_2$	char[8]	{54 65 78 74 32 00 00 00}
$Text_3$	char[8]	{54 65 78 74 33 00 00 00}
$Text_4$	char[8]	{54 65 78 74 34 00 00 00}
$Text_5$	char[8]	{54 65 78 74 35 00 00 00}

D.2.2 其他相关约定

此鉴别机制的实现，需要其他相关约定如下。

a) 本示例采用 GB/T 36624 定义的可鉴别的加密机制 5(GCM)实现，其使用的密码算法是 SM4。

b) 数据项 X 和数据项 Y 的级联结果 $X \| Y$ 采用 4.1 的“注”中 a)方式实现，即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。

c) 协议的打包格式为二进制。

d) 根据 7.3.3，可区分标识符是可选的，本示例使用I_A、I_B表示。示例中给出了这些可选参数，因此这些可选参数需全部验证。

D.2.3 机制示例描述

下面是对机制 *MUT.CR*——三次传递鉴别示例的描述。

a) B 产生一个随机数R_B并向 A 发送，同时发送一个文本字段$Text_1$给 A。

b) A 产生一个随机数R_A，然后产生$Token_{AB}$并发送给 B。其中e_{KAB}(十六进制)为：

{e8 99 a2 7f 9b 0f 53 f8 f1 51 c0 ea b0 d0 80 e7
67 e9 df 74 b2 01 89 72 fd 19 98 0a 04 b8 03 59
54 71 a3 76 f5 d0 04 8f e1 87 c1 b9 87 60 f3 8a
73 d2 ae 87 a9 2d d3 cb 17 4e 86 1a cd dd 83 06}

对应的 TAG(十六进制)为：

{d6 70 19 b0 13 29 62 7f 95 d0 7e 83 01 cc 93 6d}

A 发给 B 的$Token_{AB}$(十六进制)为：

{54 65 78 74 33 00 00 00 e8 99 a2 7f 9b 0f 53 f8
f1 51 c0 ea b0 d0 80 e7 67 e9 df 74 b2 01 89 72
fd 19 98 0a 04 b8 03 59 54 71 a3 76 f5 d0 04 8f
e1 87 c1 b9 87 60 f3 8a 73 d2 ae 87 a9 2d d3 cb
17 4e 86 1a cd dd 83 06}

c) B 收到包含$Token_{AB}$的消息，通过K_{AB}对对应的密文数据进行解密并验证数据完整性，之后验证对应数据是否符合预期。根据 7.3.3，先比较 SID，再检验e_{KAB}部分，即对比I_B和R_B是否与$Token_{AB}$中的相符。若不符合，则拒绝进一步验证，若符合则通过验证。同时计算e_{KAB}(十六进制)，计算结果如下：

{e8 99 a2 7f 9b 0f 53 f8 f2 51 c0 ea b0 d0 80 e7
67 e9 df 74 b2 01 89 72 fd 19 98 0a 04 b8 03 59
41 63 bf 6b ff d9 04 81 b5 e2 b9 cd b3 60 f3 ec}

对应的 TAG(十六进制)：

{52 f1 0b a8 e5 b4 0d f5 4b 11 6a 5e 19 ae 9b 61}

d) B 产生并向 A 发送$Token_{BA}$(十六进制)：

{54 65 78 74 35 00 00 00 e8 99 a2 7f 9b 0f 53 f8
f2 51 c0 ea b0 d0 80 e7 67 e9 df 74 b2 01 89 72
fd 19 98 0a 04 b8 03 59 41 63 bf 6b ff d9 04 81
b5 e2 b9 cd b3 60 f3 ec}

e) A 收到 B 发送的$Token_{BA}$，利用K_{AB}进行解密并验证数据完整性，之后验证对应数据是否符合预期。根据 7.3.3，先比较 SID，再检验$e_{K_{AB}}$部分，即对比I_B和R_B是否与$Token_{AB}$中的相符。若不符合，则不能进一步验证，若符合则通过验证。

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] GM/T 0103 随机数发生器总体框架

[9] GM/T 0105 软件随机数发生器设计指南

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

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

[12] 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

中 华 人 民 共 和 国

国 家 标 准

网络安全技术 实体鉴别

第2部分:采用鉴别式加密的机制

GB/T 15843.2—2024

*

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(100029)

北京市西城区三里河北街16号(100045)

网址:www.spc.net.cn

服务热线:400-168-0010

2024年9月第一版

*

书号:155066·1-77616

GB/T 15843.2-2024