ICS 35.020
L 70
备案号：37627—2012

SB

中华人民共和国国内贸易行业标准

SB/T 10769—2012

基于射频识别的瓶装酒追溯与防伪查询服务流程

Inquiring service process of bottled alcoholic beverage traceability and anti-counterfeiting based on radio frequency identification

2012-09-19 发布　　2012-12-01 实施

中华人民共和国商务部　　发布

目　　次

前言 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　符号 …… 1
5　缩略语 …… 1
6　瓶装酒生产流通过程与记录 …… 2
7　追溯查询服务流程 …… 4
8　防伪查询服务流程 …… 7
9　瓶装酒追溯与防伪命令定义 …… 8
10　UHF 标签清点识别兼容方案 …… 12
附录 A（规范性附录）　双向鉴别 …… 13
附录 B（资料性附录）　UHF 标签盘点识别兼容方案 …… 17
附录 C（资料性附录）　网络层可信安全技术 …… 18
参考文献 …… 19

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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。

本标准由中华人民共和国商务部提出并归口。

本标准起草单位：工业和信息化部电子工业标准化研究院、烟台东方瑞创达电子科技有限公司、北京中电华大电子设计有限责任公司、西安西电捷通无线网络通信有限公司、烟台张裕葡萄酿酒股份有限公司、贵州茅台酒股份有限公司、四川宜宾五粮液股份有限公司。

本标准主要起草人：宋继伟、耿力、高林、冯敬、尚红权、兰天、杜志强、何飞、张国强、费渡、张征平、金倩、王文峰、鞠远程、张睿。

基于射频识别的瓶装酒追溯与防伪查询服务流程

1 范围

本标准规定了瓶装酒追溯与防伪应用中，瓶装酒生产流通过程与记录、防伪查询服务流程、追溯查询服务流程和瓶装酒追溯与防伪命令等的要求。

本标准适用于基于射频识别的瓶装酒追溯与防伪应用系统的设计开发和使用。

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 22351.3—2008 识别卡 无触点的集成电路卡 邻近式卡 第3部分：防冲突和传输协议

SB/T 10771 基于射频识别的瓶装酒追溯与防伪应用数据编码

SB/T 10772 信息技术 射频识别 支持安全协议的800/900 MHz空中接口通信协议

3 术语和定义

下列术语和定义适用于本文件。

3.1

追溯与防伪公共服务平台 traceability and anti-counterfeiting public service platforms

作为瓶装酒追溯与防伪系统中心节点，连接读写器与酒厂数据库，接入和分发酒类追溯与防伪消息的基础信息平台。

4 符号

T_{sec}：读写器发送一个安全命令之后，等待标签响应的最大时间为20 ms 至 T_{sec}。

5 缩略语

AK——鉴别密钥(authentication key)；

CRC——循环冗余校验码(cyclic redundancy check)；

HF——高频(high frequency)；

RET——鉴别结果(result)；

RK——根密钥(root key)；

RKI——根密钥索引(root key index)；

RN——随机数(random number)；

TD——追溯数据集合(trace dataset)；

TID——标签标识符(tag identifier)；

UHF——超高频(ultra high frequency)；

UTadd——用户终端地址(user terminal address)。

6 瓶装酒生产流通过程与记录

6.1 过程组成

瓶装酒生产流通过程分为生产、库存、物流和查询4个环节，每个环节都将形成瓶装酒的数据记录并记入酒厂数据库。其中生产、库存和物流环节使用酒厂自有系统；查询环节包括管理部门的追溯查询和用户的防伪查询，查询请求由管理部门提供的追溯与防伪公共服务平台接入，并转接到酒厂数据库系统。瓶装酒生产流通过程如图1所示。

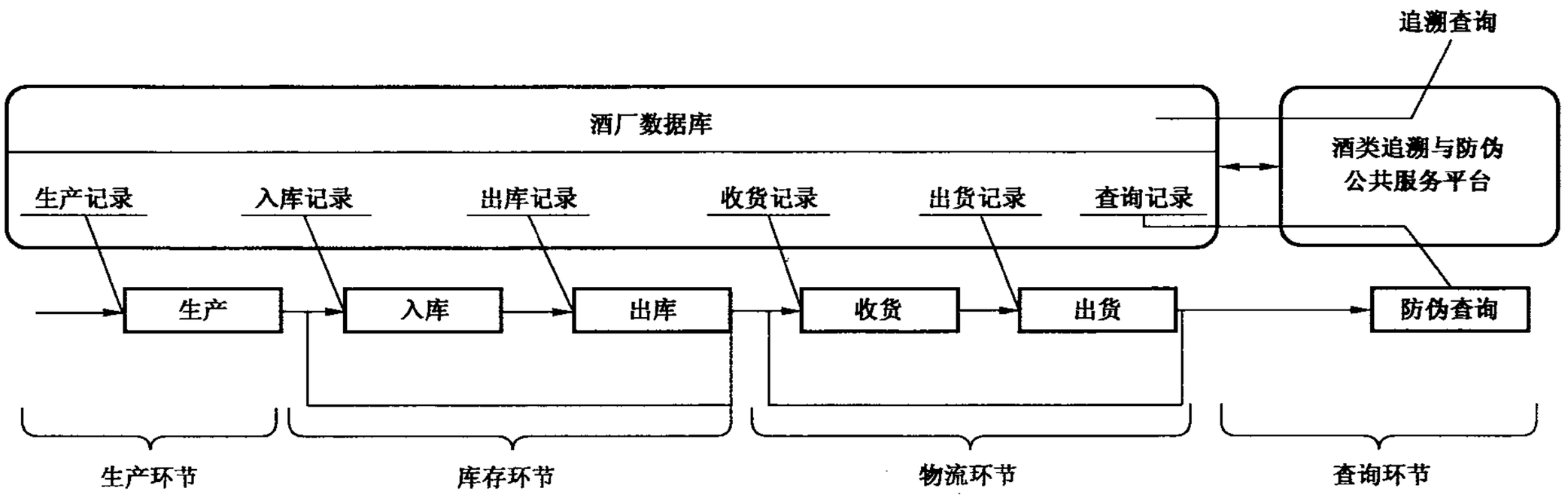

图1 瓶装酒生产流通过程

6.2 生产环节

瓶装酒生产时，应在酒厂数据库生成唯一的生产记录，该记录至少包括表1中所示的数据项，并逐项赋值。同时，应在此环节贴合瓶装酒追溯与防伪标签并写入相应数据。各数据项定义应符合SB/T 10771中相关规定。

表1 瓶装酒生产记录

环　　节	数　据　项	数据长度(字节)
生产环节	TID	8
	瓶装酒单品唯一标识符或箱体唯一标识符	16或20
	酒名称	16
	酒容量规格	2
	酒精度	1
	生产日期	4
	保质期	1
	瓶装酒包装规格	1
	生产批次	4
	酒产地	16

6.3 库存环节

6.3.1 入库

瓶装酒每次入库时，应在酒厂数据库生成唯一的入库记录，该记录至少包括表 2 中所示的数据项，并对库房号和入库时间赋值。各数据项定义应符合 SB/T 10771 中相关规定。

6.3.2 出库

瓶装酒每次出库时，对应到酒厂数据库中的入库记录，并对出库时间和下一级收货单位赋值。各数据项定义应符合 SB/T 10771 中相关规定。

表 2 瓶装酒出入库记录

环　　节	数　据　项	数据长度(字节)
库存环节	库房号	2
	入库时间	6
	出库时间	6
	下一级收货单位	16

6.4 物流环节

6.4.1 收货

瓶装酒每次收货时，应在酒厂数据库生成唯一的收货记录，该记录至少包括表 3 中所示的数据项，并对收货单位、收货单位入库时间赋值。各数据项定义应符合 SB/T 10771 中相关规定。

6.4.2 出货

瓶装酒每次出货时，对应到酒厂数据库中的出货记录，并对收货单位出库时间和下一级收货单位赋值。各数据项定义应符合 SB/T 10771 中相关规定。

表 3 瓶装酒流通记录

环　　节	数　据　项	数据长度(字节)
物流环节	收货单位	16
	收货单位入库时间	6
	收货单位出库时间	6
	下一级收货单位	16

6.5 查询环节

6.5.1 追溯查询

瓶装酒追溯查询用于管理部门对瓶装酒的流通过程进行追溯。追溯查询结果应保留在追溯与防伪公共服务平台中。

6.5.2 防伪查询

瓶装酒防伪查询用于用户进行防伪判别。每次防伪查询时，应在酒厂数据库生成唯一的防伪查询记录，该记录至少包括表 4 中所示的数据项。各数据项定义应符合 SB/T 10771 中相关规定。

表 4 瓶装酒查询记录

环　　节	数 据 项	数据长度(字节)
查询环节	查询类别	1
	查询时间	6
	读写器代码	10
	查询结果	不定长

7 追溯查询服务流程

7.1 概述

追溯查询可通过追溯和防伪读写器(以下简称读写器)自动读取或通过信息系统手工录入方式实现，服务流程如图 2 所示。

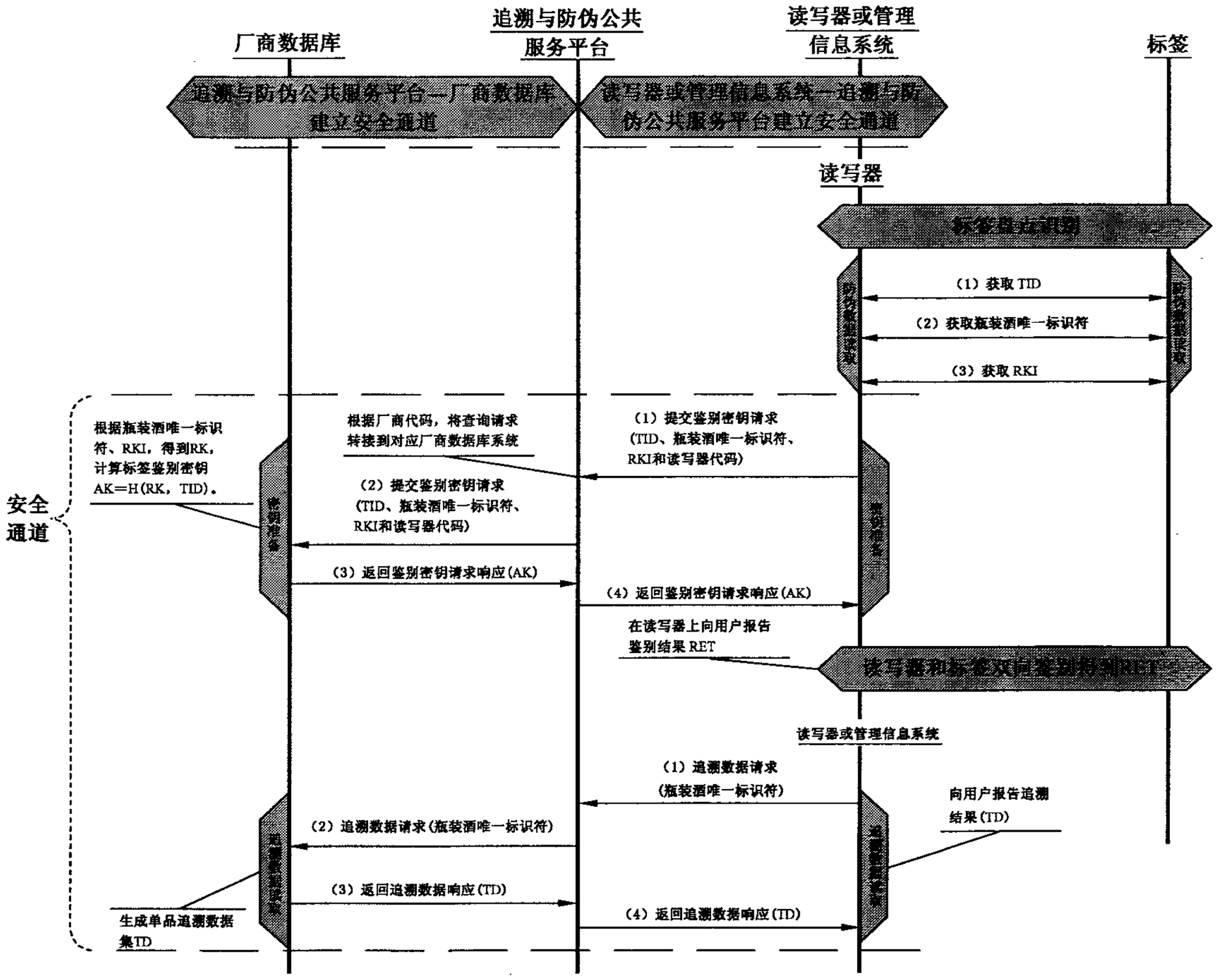

图 2 追溯查询服务流程

追溯查询服务流程包括标签盘点识别、防伪数据读取、密钥准备、读写器和标签双向鉴别与信息显示、追溯数据读取5个环节。

在执行追溯查询前，读写器与追溯和防伪公共服务平台之间、追溯和防伪公共服务平台与厂商数据库之间，都应建立安全数据传输通道，该安全数据传输通道应保证传输数据的机密性和完整性。安全数据传输通道的技术实现可参见附录C。

7.2 标签盘点识别

UHF标签盘点识别应符合SB/T 10772中相关规定；

HF标签盘点识别应符合GB/T 22351.3—2008中相关规定。

7.3 防伪数据读取

防伪数据读取用于获取后续防伪鉴别所需的TID、瓶装酒单品唯一标识符或箱体唯一标识符和RKI。

UHF标签的上述数据读取流程应符合SB/T 10772中相关规定；

HF标签的上述数据读取流程应符合GB/T 22351.3—2008中相关规定。

7.4 密钥准备

读写器使用得到的TID、瓶装酒单品唯一标识符或箱体唯一标识符、RKI和读写器代码，构造鉴别密钥请求，发送到追溯与防伪公共服务平台。

追溯与防伪公共服务平台收到鉴别密钥请求后，从瓶装酒单品唯一标识符或箱体唯一标识符中得到厂商代码，根据厂商代码选择对应厂商的数据库系统，并转发该鉴别密钥请求。

厂商数据库系统得到鉴别密钥请求后，利用瓶装酒单品唯一标识符或箱体唯一标识符和RKI，查找得到RK；再根据TID，利用散列算法计算出AK=H(RK,TID)，其中H为散列算法。然后利用AK构造鉴别密钥响应，并发送到追溯与防伪公共服务平台。

追溯与防伪公共服务平台收到鉴别密钥响应后，转发到读写器。

读写器收到鉴别密钥响应后，得到其中的AK。

7.5 读写器和标签双向鉴别与信息显示

读写器根据得到的AK与标签进行双向身份鉴别；

UHF标签和读写器鉴别过程应符合SB/T 10772 6.6.3中相关规定；

HF标签和读写器鉴别过程见附录A。

读写器得到双向鉴别结果后，从标签中读取该瓶装酒的基本信息，利用读写器的显示装置，显示该基本信息和验证结果，显示内容至少包括表5中所示数据项。

表5 瓶装酒防伪查询结果

数据项	数据长度(字节)	备　　注
瓶装酒单品唯一标识符或箱体唯一标识符	16或20	定义见SB/T 10771中5.3
酒名称	16	—
酒容量规格	2	单位：mL
酒精度	1	单位：度

表 5（续）

数据项	数据长度(字节)	备　　注
生产日期	4	—
保质期	4	单位:月
验证结果	10	如果鉴别被成功执行且验证通过,则显示瓶装酒的基本要素信息和“有此记录”; 如果鉴别被成功执行但验证未通过,则显示“查无此记录,谨防假冒”。

7.6　追溯数据读取

在读写器追溯方式下,读写器完成对标签的验证,如果有此记录,则进行追溯数据读取;否则流程终止。在管理信息系统追溯方式下,录入瓶装酒单品唯一标识符或箱体唯一标识符进行追溯数据读取。

读写器或管理信息系统根据得到的瓶装酒单品唯一标识符或箱体唯一标识符,构造追溯数据请求,并发送给追溯与防伪公共服务平台,并将该请求转发到相应的厂商数据库中。

厂商数据库收到追溯请求后,生成单品的 TD,构造追溯数据响应,并返回给追溯与防伪公共服务平台,并将该响应转发到读写器或管理信息系统。

读写器或管理信息系统收到追溯数据响应后,应在显示装置上显示至少包括表 6 中所示数据项。

表 6　瓶装酒追溯查询结果

数　据　项		数据长度(字节)	备　注
生产环节	TID	8	—
	瓶装酒单品唯一标识符或箱体唯一标识符	16 或 20	见 SB/T 10771 中 5.3
	酒名称	16	—
	酒容量规格	2	单位:mL
	酒精度	1	单位:度
	生产日期	4	—
	保质期	1	单位:月
	瓶装酒包装规格	1	—
	生产批次	4	—
	酒产地	16	—
库存环节 1	库房号	2	—
	入库时间	6	—
	出库时间	6	—
	下一级收货单位	16	—
库存环节 2..n	库房号	2	—
	入库时间	6	—
	出库时间	6	—
	下一级收货单位	16	—

表 6（续）

数　据　项		数据长度(字节)	备　注
物流环节 1	收货单位	16	—
	收货单位入库时间	6	—
	收货单位出库时间	6	—
	下一级收货单位	16	—
物流环节 2..m	收货单位	16	—
	收货单位入库时间	6	—
	收货单位出库时间	6	—
	下一级收货单位	16	—

8　防伪查询服务流程

8.1　概述

防伪查询应通过读写器自动读取方式实现，防伪查询服务流程如图 3 所示。

整个防伪查询服务流程包括标签盘点识别、防伪数据读取、密钥准备、读写器和标签双向鉴别与信息显示、查询结果记录、用户通告 6 个环节，其中用户通告为可选环节。

在执行防伪查询前，读写器与追溯和防伪公共服务平台之间、追溯和防伪公共服务平台与厂商数据库之间，都应建立安全数据传输通道，该安全数据传输通道应保证传输数据的机密性和完整性。安全数据传输通道的技术实现可参见附录 C。

在用户通告环节，追溯与防伪公共服务平台可利用独立第三方通道，将防伪查询结果通告给用户独立终端。

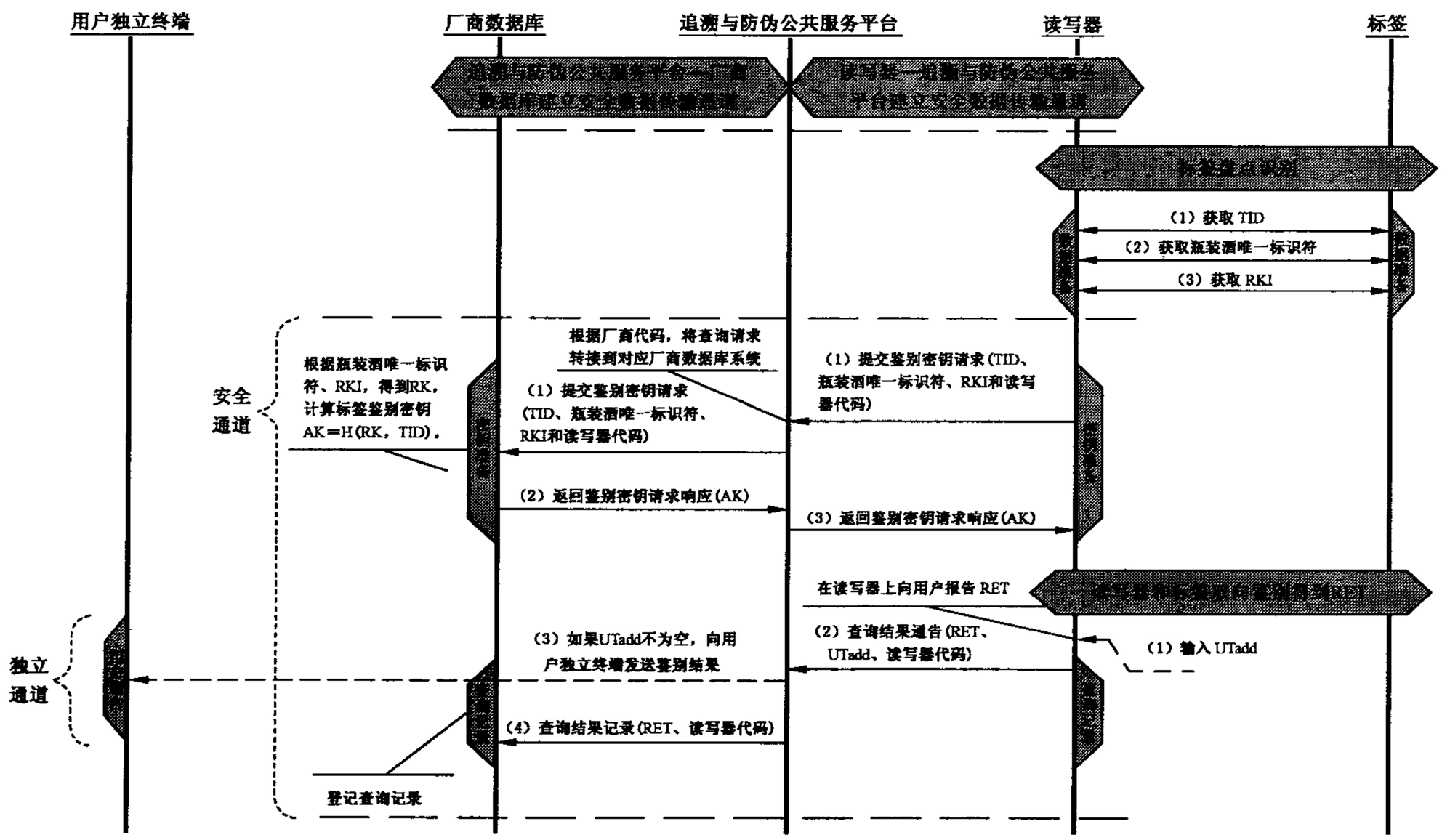

图 3　防伪查询服务流程

8.2 标签盘点识别

见 7.2。

8.3 防伪数据读取

见 7.3。

8.4 密钥准备

见 7.4。

8.5 读写器和标签的双向鉴别与信息显示

见 7.5。

8.6 查询结果记录和用户通告

读写器和标签完成双向鉴别后，利用读写器的显示装置，向用户显示该瓶装酒的基本信息和防伪查询结果。同时构造查询结果通告，发送给追溯与防伪公共服务平台。追溯与防伪公共服务平台收到查询结果通告后，构造查询结果记录，并发送给厂商数据库系统。厂商数据库系统收到该记录后，生成查询记录并存储到厂商数据库中。

如果用户需要确认查询结果，应在读写器中输入 UTadd，UTadd 包含在查询结果通告命令中，追溯与防伪公共服务平台在查询结果通告中得到 UTadd 后，通过独立第三方通道将查询结果发送到用户终端上，以供用户确认。该查询结果至少包括表 6“生产环节”中除“TID”和“瓶装酒单品唯一标识符或箱体唯一标识符”外的数据项。

8.7 脱机防伪查询

受控管理读写器应支持脱机防伪查询功能。具有脱机防伪查询功能的读写器，应存储鉴别 RK 和必要数据，实现标签盘点识别、防伪数据读取、密钥准备和双向鉴别功能。在具有联网条件时，读写器离线记录的查询结果应上传到追溯与防伪公共服务平台。脱机防伪查询不支持“用户通告”功能。

9 瓶装酒追溯与防伪命令定义

9.1 命令列表

瓶装酒追溯与防伪命令见表 7。

表 7 瓶装酒追溯与防伪命令

命令范围	环节	操作命令	命令功能描述	备注
追溯查询和防伪查询中的共有命令	标签盘点识别	—	—	[a]
	防伪数据读取	—	—	[a]
	密钥准备	鉴别密钥请求（skReq）	读写器发给追溯与防伪公共服务平台，追溯与防伪公共服务平台发给厂商数据库；用于请求鉴别用的鉴别密钥。	见 7.4
		鉴别密钥响应（skRsp）	厂商数据库发给追溯与防伪公共服务平台，追溯与防伪公共服务平台发给读写器；用于返回鉴别用的鉴别密钥。	见 7.4

表 7（续）

命令范围	环节	操作命令	命令功能描述	备注
追溯查询和防伪查询中的共有命令	双向鉴别	安全参数获取	读写器发给标签； 用于获得标签的安全配置信息。	[b]
		身份鉴别	读写器和标签进行双向身份鉴别	[b]
追溯查询中的命令	追溯数据读取	追溯数据请求（tdReq）	读写器或管理信息系统发给追溯与防伪公共服务平台，追溯与防伪公共服务平台发给厂商数据库； 用于向厂商数据库请求追溯数据。	见 7.6
	追溯数据读取	追溯数据响应（tdRsp）	厂商数据库发给追溯与防伪公共服务平台，追溯与防伪公共服务平台发给读写器或管理信息系统； 用于向读写器或管理信息系统返回追溯数据。	见 7.6
防伪查询中的命令	查询结果记录与用户通告	查询结果通告（retNtf）	读写器发给追溯与防伪公共服务平台； 用于向追溯与防伪公共服务平台通告鉴别结果。	见 8.6
		查询过程记录（qryReg）	追溯与防伪公共服务平台发给厂商数据库； 用于向厂商数据库通告查询结果， 并在厂商数据库中写入查询记录。	见 8.6

[a] UHF 标签应符合 SB/T 10772 中相关命令；HF 标签应符合 GB/T 22351.3 中相关命令。

[b] UHF 标签应符合 SB/T 10772 6.6.3 中相关命令；HF 标签应符合附录 A 中相关命令。

9.2 命令编码规则

瓶装酒追溯与防伪命令采用 XML 编码格式，分请求与响应两个部分，如图 4、图 5 所示。

```
〈? xml version="1.0" encoding="utf-8" ?〉
〈ta〉
    〈request id="{命令编码}" name="{命令名称}"〉
        〈parameters〉
            〈parameter name="{参数名称}" type="{参数类型}"〉{参数值}〈/parameter〉
            ……
        〈/parameters〉
    〈/request〉
〈/ta〉
```

图 4 瓶装酒追溯与防伪命令 XML 编码格式请求部分

```
〈? xml version="1.0" encoding="utf-8" ?〉
〈ta〉
    〈response id="{命令编码}" name="{命令名称}"〉
        〈result id="{结果编码}"〉{结果描述}〈/result〉
        〈parameters〉
            〈parameter name="{参数名称}" type="{参数类型}"〉{参数值}〈/parameter〉
            ……
        〈/parameters〉
    〈/response〉
〈/ta〉
```

图 5　瓶装酒追溯与防伪命令 XML 编码格式响应部分

命令中相关要素说明如下：

a）　命令编码和命令名称：用于标识请求或响应的命令；

b）　参数名称、参数类型和参数值：用于标识请求或响应的参数，具体定义如 9.3 所示；

c）　结果编码和结果描述：用于标识响应结果的状态。结果编码为 0 表示成功，为其他值表示失败；结果描述用于对结果进行进一步说明。

9.3　命令详细定义

9.3.1　鉴别密钥请求(skReq)

鉴别密钥请求命令定义如图 6 所示。

```
〈? xml version="1.0" encoding="utf-8" ?〉
〈ta〉
    〈request id="1" name="skReq"〉
        〈parameters〉
            〈parameter name="TID" type="string"〉{标签标识符}〈/parameter〉
            〈parameter name="UII" type="string"〉{瓶装酒单品唯一标识符或箱体唯一标识符}〈/parameter〉
            〈parameter name="RKI" type="string"〉{根密钥索引}〈/parameter〉
        〈/parameters〉
    〈/request〉
〈/ta〉
```

图 6　鉴别密钥请求命令

9.3.2　鉴别密钥响应(skRsp)

鉴别密钥响应命令定义如图 7 所示。

```
〈? xml version="1.0" encoding="utf-8" ?〉
〈ta〉
    〈response id="2" name="skRsp"〉
        〈result id="{结果编码}"〉{结果描述}〈/result〉
        〈parameters〉
            〈parameter name="AK" type="string"〉{鉴别密钥}〈/parameter〉
        〈/parameters〉
    〈/response〉
〈/ta〉
```

图 7　鉴别密钥响应命令

9.3.3 查询结果通告(retNtf)

查询结果通告命令定义如图 8 所示。

```
〈? xml version="1.0" encoding="utf-8" ?〉
〈ta〉
    〈request id="3" name="retNtf"〉
        〈parameters〉
            〈parameter name="utadd" type="string"〉{用户终端地址}〈/parameter〉
            〈parameter name="result" type="string"〉{查询结果}〈/parameter〉
            〈parameter name="readercode" type="string"〉{读写器代码}〈/parameter〉
        〈/parameters〉
    〈/request〉
〈/ta〉
查询结果:0x01 查询到该记录，0x00 未查询到该记录
```

图 8 查询结果通告命令

9.3.4 查询过程记录(qryReg)

查询过程记录命令定义如图 9 所示。

```
〈? xml version="1.0" encoding="utf-8" ?〉
〈ta〉
    〈request id="4" name="qryReg"〉
        〈parameters〉
            〈parameter name="result" type="string"〉{查询结果}〈/parameter〉
            〈parameter name="readercode" type="string"〉{读写器代码}〈/parameter〉
        〈/parameters〉
    〈/request〉
〈/ta〉
查询结果:0x01 查询到该记录，0x00 未查询到该记录
```

图 9 查询过程记录命令

9.3.5 追溯数据请求(bwDataReq)

追溯数据请求命令定义如图 10 所示。

```
〈? xml version="1.0" encoding="utf-8" ?〉
〈ta〉
    〈request id="5" name="bwDataReq"〉
        〈parameters〉
            〈parameter name="UII" type="string"〉{瓶装酒单品唯一标识符或箱体唯一标识符}〈/parameter〉
            〈parameter name="batchnumber" type="string"〉{生产批次编号}〈/parameter〉
        〈/parameters〉
    〈/request〉
〈/ta〉
```

图 10 追溯数据请求命令

9.3.6 追溯数据响应(bwDataRsp)

追溯数据响应命令定义如图 11 所示。

```
〈? xml version="1.0" encoding="utf-8" ?〉
〈ta〉
〈response id="6" name="bwDataRsp"〉
        〈result id="{结果编码}"〉{结果描述}〈/result〉
        〈parameters〉
                〈parameter name="TID" type="string"〉{标签标识符}〈/parameter〉
                〈parameter name="UII" type="string"〉{瓶装酒单品唯一标识符或箱体唯一标识符}〈/parameter〉
                〈parameter name="productionname" type="string"〉{酒名称}〈/parameter〉
                〈parameter name="content" type="string"〉{酒容量规格}〈/parameter〉
                〈parameter name="degree" type="string"〉{酒精度}〈/parameter〉
                〈parameter name="productiondate" type="string"〉{生产日期}〈/parameter〉
                〈parameter name="batchnumber" type="string"〉{生产批次}〈/parameter〉
                〈parameter name="qualityperiod" type="string"〉{保质期}〈/parameter〉
                〈parameter name="specification" type="string"〉{瓶装酒包装规格}〈/parameter〉
                〈parameter name="productionplace" type="string"〉{酒产地}〈/parameter〉
                〈parameter name="stockcount" type="number"〉{库存环节数量(记为 n)}
〈/parameter〉
                〈parameter name="stock" type="string"〉
                    {库房号,入库时间，出库时间，下一级收货单位}〈/parameter〉
                    2..n 个库存环节数据
                〈parameter name="flowcount" type="number"〉{流通环节数量(记为 m)}〈/parameter〉
                    〈parameter name="flow" type="string"〉
                    {收货单位，收货单位入库时间，收货单位出库时间，下一级收货单位}〈/parameter〉
                    2..m 个流通环节数据
                〈/parameters〉
        〈/response〉
〈/ta〉
```

图 11 追溯数据响应命令

9.4 瓶装酒追溯与防伪命令间时序

应保证瓶装酒追溯与防伪命令间时序的完整性,并具有命令超时应对机制。

10 UHF 标签清点识别兼容方案

参见附录 B。

附 录 A
（规范性附录）
双 向 鉴 别

A.1 双向鉴别流程

本标准定义的双向鉴别完整流程包括如下两个阶段：

——鉴别数据获取阶段，用于获得鉴别用的数据，为后续鉴别协议做准备；

——双向鉴别阶段，用于完成读写器和标签的双向鉴别。

鉴别数据获取阶段提供一种安全协商机制，使读写器获得标签的安全配置，并使用匹配的安全配置和标签进行通信。当读写器已知标签安全配置时，该阶段可以跳过直接进行双向鉴别。

鉴别数据获取阶段通过安全参数获取命令(GetSecPara)实现，读写器发出安全参数获取命令，标签返回相应的安全参数。

双向鉴别通过如下命令实现：

——读写器发出鉴别请求命令(ReqAuth)，标签返回 32 位随机数数据 R_t；

——读写器发出鉴别命令(Token1)，标签返回应答数据 Token2。

流程如图 A.1 所示：

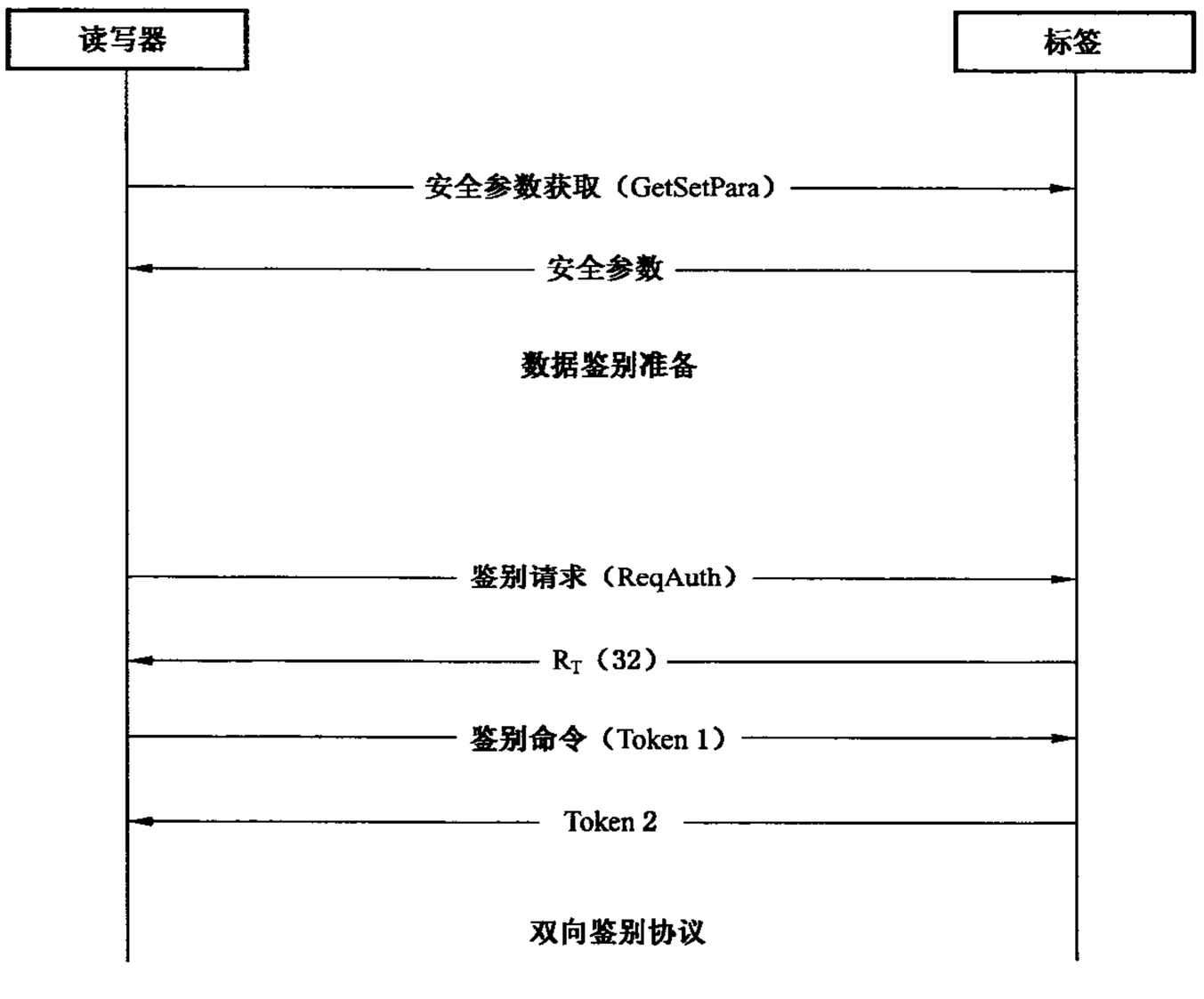

图 A.1 双向鉴别流程

具体流程步骤描述如下：

a) 读写器发送安全参数获取命令，标签收到该命令后，提取内部存储的安全参数返回给读写器，安全参数包括密码算法、密钥长度、单/双向鉴别、RKI。

b) 读写器发出鉴别请求命令，标签返回 32 位随机数 R_T。

c) 读写器收到 R_T 后产生 32 位随机数 R_R，之后进行第一次分组加密运算，加密的明文为 $R_R||R_T$，生成密文，发送鉴别命令 Token1。

d) 标签接收 Token1 之后进行算法解密得到明文，其中的高 32 位内容为 R_R'，低 32 位内容为 R_T'。比较 R_T'与 R_T，如果 R_T'与 R_T 不一致，则鉴别不通过；如果 R_T'与 R_T 一致，则标签再进行一次分组加密运算，加密的明文为 TID 低 32 位和 R_R'，加密后产生密文 Token2，返回给读写器。

e) 读写器接收到 Token2 后做解密运算，得到明文的低 32 位内容记为 R_R"。比较 R_R"和 R_R，如果 R_R"与 R_R 一致，鉴别通过。如果 R_R"与 R_R 不一致，则鉴别不通过。

A.2 双向鉴别命令定义

A.2.1 获取安全参数命令

获取安全参数命令见表 A.1。

表 A.1 获取安全参数命令

命令格式	命令码	RN	CRC
位数	8	16	16
描述	11001100_b	句柄	CRC-16

标签对获取安全参数命令的响应见表 A.2。该响应包含从用户子区数量、存储区属性、安全参数、RKI、RN 计算得到的 CRC-16。

表 A.2 标签对获取安全参数命令的响应

数据格式	保留	安全参数	RN	CRC
位数	20	32	16	16
描述	保留	—	句柄	CRC-16

安全参数字段定义见表 A.3。

表 A.3 安全参数字段定义

	b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}
安全参数	RKI															
	b_{16}	b_{17}	b_{18}	b_{19}	b_{20}	b_{21}	b_{22}	b_{23}	b_{24}	b_{25}	b_{26}	b_{27}	b_{28}	b_{29}	b_{30}	b_{31}
	密码算法			密钥长度		安全功能			保留	T_{sec}						

密码算法字段定义见表 A.4。

表 A.4 密码算法字段

密码算法	描　　述
000_b	保留
001_b	保留

表 A.4（续）

密码算法	描　　述
010_b	对称密码算法
011_b-111_b	保留

密钥长度字段定义见表 A.5。

表 A.5　密钥长度字段

密钥长度	描　　述
00_b	32 位
01_b	64 位
10_b	128 位
11_b	保留

安全功能字段定义见表 A.6。

表 A.6　安全功能字段

密钥长度	描　　述
000_b	对标签单向鉴别
001_b	对读写器单向鉴别
010_b	双向鉴别
其他	保留

RKI 字段为对散列出本标签鉴别密钥的 RK 索引值，能够唯一标识一个 RK，读写器根据该索引获取 RK 和标签完成身份鉴别。

A.2.2　鉴别请求命令

该命令为读写器请求鉴别认证的指令，标签在确认状态下收到该指令后，进入鉴别状态。

读写器发送的命令帧格式见表 A.7。

表 A.7　读写器发送的命令帧格式

命令格式	命令码	RN	CRC-16
位数	16	16	16
描述	11100000_b_00000010_b	16 位随机数	—

标签返回的响应帧格式见表 A.8。

表 A.8　标签返回的响应帧格式

响应格式	参数	数据	随机数	CRC-16
位数	16	96	16	16
描述	RKI	TID	句柄	—
句柄为命令帧的 RN。				

A.2.3　鉴别命令

读写器分两次发送身份鉴别指令。标签只在鉴别状态下，能够处理鉴别指令。

读写器第一次发送的指令帧格式见表 A.9。

表 A.9　读写器第一次发送的指令帧格式

命令格式	命令码	参数	随机数	CRC-16
位数	16	8	16	16
描述	11100000_b_00000001_b	0000_0000_b	句柄	—

标签第一次返回的响应帧格式见表 A.10。

表 A.10　标签第一次返回的响应帧格式

响应格式	随机数	随机数	CRC-16
位数	32	16	16
描述	R_T	句柄	—
R_T 为标签产生的 32 位随机数。			

读写器第二次发送的指令帧格式见表 A.11。

表 A.11　读写器第二次发送的指令帧格式

命令格式	数据	随机数	CRC-16
位数	64	16	16
描述	Token1	句柄	—
Token1＝Enc(R_R||R_T,KEY)。			

标签第二次返回的响应帧格式见表 A.12。

表 A.12　标签第二次返回的响应帧格式

响应格式	数据	随机数	CRC-16
位数	64	16	16
描述	Token2	句柄	—
Token2＝Enc(R_T"||R_R',KEY)。			

附 录 B
（资料性附录）
UHF 标签盘点识别兼容方案

B.1 兼容多种空中接口协议的瓶装酒防伪标签盘点识别流程如图 B.1 所示。

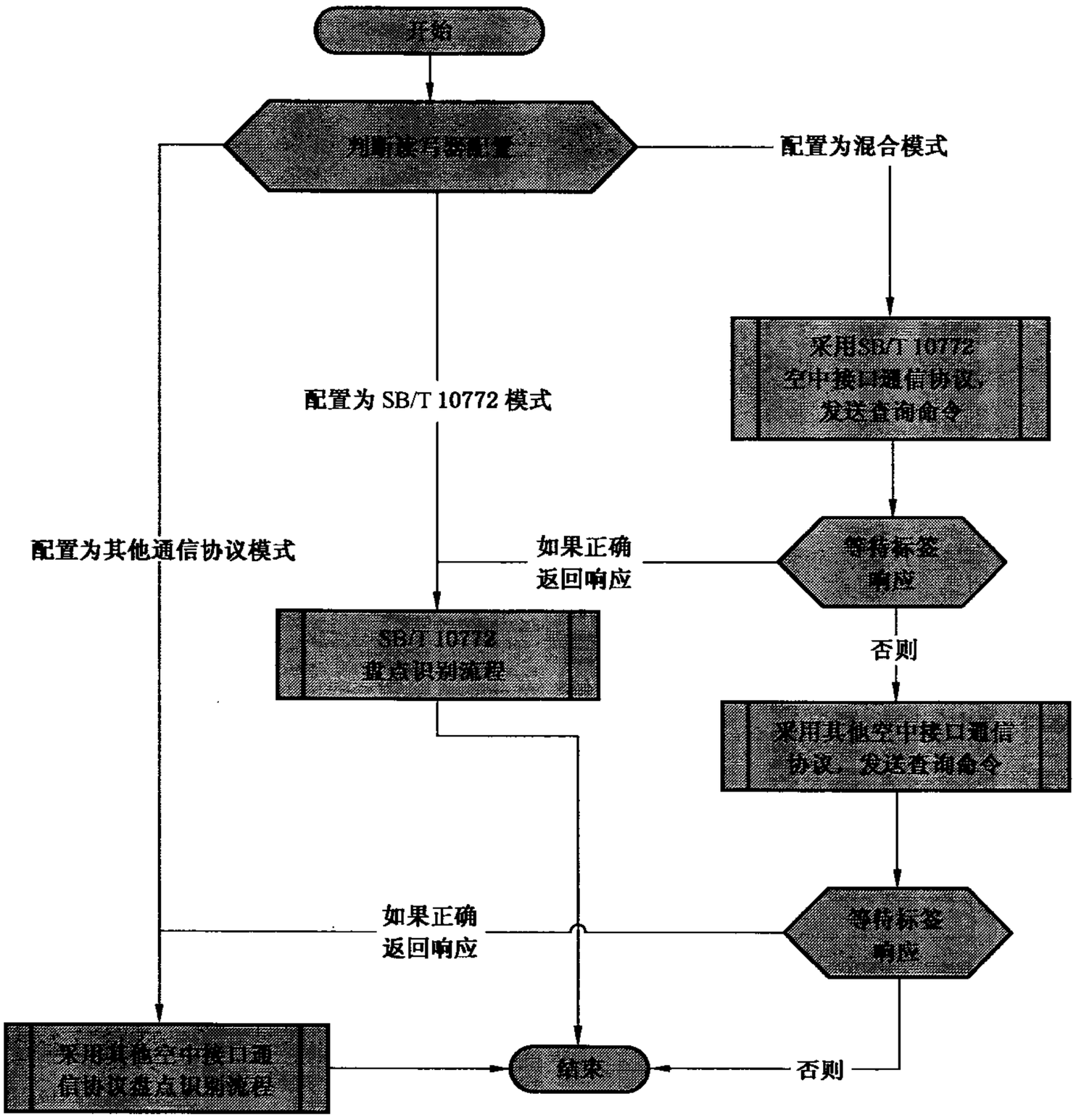

图 B.1 标签盘点识别流程

附 录 C
（资料性附录）
网络层可信安全技术

C.1 网络层可信安全技术用于提供身份鉴别的可信安全框架，可参见 ISO/IEC 9798-3：1998/Amd.1：2010。

参 考 文 献

[1] ISO/IEC 9798-3:1998/Amd.1:2010 信息技术 安全技术 实体鉴别 第3部分:使用数字签名技术的机制 补篇1(Information technology—Security techniques—Entity authentication—Part 3:Mechanisms using digital signature techniques—Amendment 1)