ICS 35.040
A 90

中华人民共和国国家标准

GB/T 38563—2020

基于移动互联网的防伪溯源验证通用技术条件

General technical requirements for anti-counterfeiting traceability verification based on mobile internet

2020-03-06 发布　　2020-10-01 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。

本标准由全国防伪标准化技术委员会(SAC/TC 218)提出并归口。

本标准起草单位:中国防伪行业协会、中防验证(北京)网络服务平台股份有限公司、北京舜天龙兴信息技术有限公司、深圳链云信息科技有限公司、北京百度网讯科技有限公司、上海市防伪技术产品测评中心、四川万识科技有限公司、中防智慧(北京)科技有限公司、湖南惠农科技有限公司。

本标准主要起草人:隆亮、陈锡蓉、刘俊宏、李龙杰、徐家军、荆博、罗隽、耿晓桦、张晋豪、孙冰、谢浩、申斌。

基于移动互联网的防伪溯源验证 通用技术条件

1 范围

本标准规定了移动互联网环境下防伪溯源验证的验证终端、验证接口、符合性、交互、安全、性能和防伪验证安全级别的要求以及试验方法。

本标准适用于基于移动互联网的防伪溯源验证，也适用于对防伪溯源验证的测试评价。

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 19425—2003 防伪技术产品通用技术条件

GB/T 22258—2008 防伪标识通用技术条件

GB/T 34062—2017 防伪溯源编码技术条件

GB/T 34975—2017 信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法

GB/T 37025—2018 信息安全技术 物联网数据传输安全技术要求

ISO/IEC 15693-2 识别卡 非接触集成电路卡 邻近卡 第2部分：空中接口和初始化(Identification cards—Contactless integrated circuit cards—Vicinity cards—Part 2：Air interface and initialization)

ISO/IEC 24791-5 信息技术 项目管理用射频识别(RFID) 软件系统基础设施 第5部分：设备接口[Information technology—Radio frequency identification (RFID) for item management—Software system infrastructure—Part 5：Device interface]

3 术语和定义

下列术语和定义适用于本文件。

3.1

移动互联网 mobile internet

采用移动无线通信方式实现的业务和服务。

3.2

防伪验证 anti-counterfeiting verification

对防伪识别特征或防伪溯源编码进行识别的过程。

3.3

基于移动互联网的防伪验证 anti-counterfeiting verification based on mobile internet

采用移动智能终端，通过移动无线通信方式进行防伪验证的过程。

3.4

移动智能终端 smart mobile terminal

接入公众移动通信网络、具有操作系统、可由用户自行安装和卸载应用软件的移动通信终端产品。

[GB/T 34975—2017，定义 3.1]

3.5

验证终端　verification terminal

用于进行防伪溯源验证的移动智能终端。

注：包括智能手机、笔记本电脑、平板电脑、移动数据终端(PDA)和专用移动防伪验证终端等。

3.6

防伪溯源　anti-counterfeiting traceability

采用防伪技术或措施，实现标的物与标识信息一一绑定，具有防复制、防转移和防篡改能力的溯源。

3.7

多媒体数字信息核验防伪系统　computer science based multichannel anti-counterfeiting product

一种综合运用编码技术、数字加密技术、网络通信技术、计算机技术的识别验证防伪溯源编码的信息系统。

[GB/T 34062—2017，定义 3.1.3]

3.8

防伪溯源编码　anti-counterfeiting traceability code

满足唯一性和随机性检测要求，按照一定规则编制并能够用于标识与唯一识别物品(产品、票证等)对象，以实现防伪溯源的数字和字符编码。

[GB/T 34062—2017，定义 3.1.1]

3.9

二维码　two-dimension code

在二维方向上都表示信息的条码符号。

[GB/T 33993—2017，定义 3.1]

4　缩略语

下列缩略语适用于本文件。

APP：应用程序(Application)

HTTPS：超文本传输安全协议(Hyper Text Transfer Protocol Secure)

ID：标识(Identifier)

JSON：对象简谱(JavaScript Object Notation)

NFC：近场通信(Near Field Communication)

RAS：带状态位的防伪射频识别技术(RFID for Anti-fake with Status)

RFID：射频识别技术(Radio Frequency Identification)

SDK：软件开发工具包(Software Development Kit)

SSL：安全套接层(Secure Sockets Layer)

UID：唯一标识(Unique Identifiers)

5　要求

5.1　验证终端

验证终端应符合表 1 要求。

表 1　验证终端要求

防伪验证方式	要　求
摄像头识别	具有摄像头功能，具备相应识别软件（包括扫码识别、图像识别、数字水印识别、视频识别等）运行系统环境，支持进行互联网查验，可实现防伪溯源码解码或图像解码功能
NFC 通信识别	具有 NFC 功能，具备相应识别软件（包括 RFID 识别、NFC 识别等功能）运行系统环境，支持进行互联网查验

5.2　验证接口

5.2.1　通用要求

防伪溯源验证服务应设置标准对外防伪验证和产品信息溯源接口，与公共平台实现对接，其接口应符合 GB/T 34062—2017 中附录 D 的要求并参考 GB/T 34062—2017 的附录 E。接口对接实现流程参见附录 A。

5.2.2　接口协议

验证接口应同时满足如下要求：

a）　字符统一采用 UTF-8 字符编码；

b）　采用 GET/POST 方法提交；

c）　签名算法采用 MD5/HMAC-SHA256 或相关国家标准签名算法，请求和返回的数据都应带上签名信息。

5.2.3　验证接口性能

验证接口性能应符合表 2 要求。

表 2　验证接口性能

项目	要求
响应时间	响应时间≤10 s
识别准确率	无污损图片的识别成功率≥99%
接口数据格式	提供接口验证的，需要返回 JSON 格式的数据，其反馈数据示例参见附录 B
图片或视频支持格式	图片验证应支持 jpg 和 png 等多种图片格式的验证； 视频验证应提供支持多种视频格式验证的接口

5.3　符合性

5.3.1　数码

防伪数码的编码及读取应符合 GB/T 34062—2017 的要求。

5.3.2　二维码

二维码的编码和读取应符合 GB/T 34062—2017 的要求。

5.3.3 RFID

RFID的编码和读取应符合GB/T 34062—2017和ISO/IEC 24791-5的要求。

5.4 交互

5.4.1 交互页面和操作

交互页面应简明，操作简便，必要时应有图文提示防伪验证操作方式。

5.4.2 验证展示内容

5.4.2.1 必要展示内容

包括验证结果、产品关键信息、第三方公共平台公信监管信息及投诉链接和联系方式。其字段及说明参见附录C。验证结果和产品关键信息按照验证是否通过分别为：

a) 验证通过时，应展示的产品关键信息包括产品名称、规格参数、生产企业、品牌、生产日期和个性物理特征照片；

b) 验证不通过时，应提示该产品为疑似假冒等相关信息。

5.4.2.2 扩展展示内容

包括防伪验证技术服务方信息、产品溯源信息、产品质量检验信息、产品唯一性的进一步核验途径、操作提示以及其他与产品相关的展示信息。其字段及说明参见附录D。

5.5 安全

5.5.1 APP

应符合GB/T 34975—2017中4.1的要求。

5.5.2 数据传输

数据传输安全应符合GB/T 37025—2018的规范。传输过程应使用SSL，应采用HTTPS协议。服务端可使用CA证书防止中间人篡改，客户端应验证CA证书。

5.5.3 数据载体

5.5.3.1 数码

数码载体安全应符合GB/T 19425—2003中的要求。

5.5.3.2 二维码

二维码载体安全应符合GB/T 34062—2017中第7章的要求。

5.5.3.3 RFID

RFID标签和RAS标签应具有唯一性，每个标签应具有唯一UID。RFID标签和RAS标签的密码应具有唯一性，不可重复使用。RFID标签和RAS标签应与商品一一绑定，满足防转移要求。

5.5.4 区块链

可采用区块链技术对防伪数据等信息进行存证，其区块链实施要求参见附录E。

5.6 性能

5.6.1 数码

数码的性能要求应符合 GB/T 19425—2003 中的规定。

5.6.2 二维码

二维码的性能要求应符合 GB/T 34062—2017 中的规定。

5.6.3 RFID

RFID 的性能要求应符合 ISO/IEC 15693-2 中的规定。

5.7 防伪验证安全级别

防伪验证安全分级见表 3。

表 3 防伪验证安全级别

安全级别	要求
A	防伪验证技术符合 GB/T 19425—2003 要求； 防伪溯源编码符合 GB/T 34062—2017 要求； 采用区块链进行存证
B	防伪验证技术符合 GB/T 19425—2003 要求； 防伪溯源编码符合 GB/T 34062—2017 要求
C	防伪验证技术符合 GB/T 19425—2003 要求

6 试验方法

6.1 试验条件

试验环境温度：(23±5)℃，试验环境相对湿度：(50±10)%。

6.2 验证接口

6.2.1 通用要求

按照 GB/T 34062—2017 中附录 D 规定的方法进行检验并参考 GB/T 34062—2017 的附录 E。

6.2.2 接口协议

审查开发者提供的接口协议。

6.2.3 验证接口规范

验证接口规范检验要求为：

a) 响应时间：使用秒表测量检验；

b) 识别准确率：准备无污损图片 100 张上传验证；

c) 接口格式：参考附录 A 的方法进行检验；

d) 图片或视频支持格式：准备 jpg、png 等图片格式进行验证，准备 MP4、MOV、MKV 等视频格式进行验证。

6.3 符合性

6.3.1 数码

由审查开发者提供的数据，按照 GB/T 34062—2017 中 6.8.1 规定的方法进行检验。

6.3.2 二维码

由审查开发者提供的数据，按照 GB/T 34062—2017 中 6.8.3 规定的方法进行检验。

6.3.3 RFID

由审查开发者提供的数据，按照 GB/T 34062—2017 中 6.8.2 规定的方法进行符合性检验，按照 ISO/IEC 24791-5 规定的方法进行兼容性检验。

6.4 交互

6.4.1 交互页面和操作

审查开发者提供的交互页面并进行防伪验证。

6.4.2 验证展示内容

6.4.2.1 必要展示内容

参照附录 C，审查开发者提供的验证内容进行验证并以秒表计时。

6.4.2.2 扩展展示内容

参照附录 D，审查开发者提供的验证内容进行验证。

6.5 安全检验

6.5.1 APP

按照 GB/T 34975—2017 中 5.1 规定的方法进行检验。

6.5.2 数据传输

按照 GB/T 37025—2018 规定的方法进行检验。

6.5.3 数据载体

6.5.3.1 数码

按照 GB/T 19425—2003 规定的方法进行检验。

6.5.3.2 二维码

按照 GB/T 34062—2017 中 7.1 规定的方法进行检验。

6.5.3.3 RFID

按照 GB/T 22258—2008 规定的方法进行检验。

6.5.4 区块链

参照附录 E，使用区块链技术进行检验。

6.6 性能检验

6.6.1 数码

按照 GB/T 19425—2003 规定的方法进行检验。

6.6.2 二维码

按照 GB/T 34062—2017 中第 7 章规定的方法进行检验。

6.6.3 RFID

按照 ISO/IEC 15693-2 规定的方法进行检验。

6.7 防伪验证安全级别

按照 GB/T 19425—2003，以及 GB/T 34062—2017 中 6.3、6.4、6.5、6.6 规定的方法进行检验。

附 录 A
（资料性附录）
接口对接实现流程

防伪溯源验证接口对接实现流程见图 A.1。

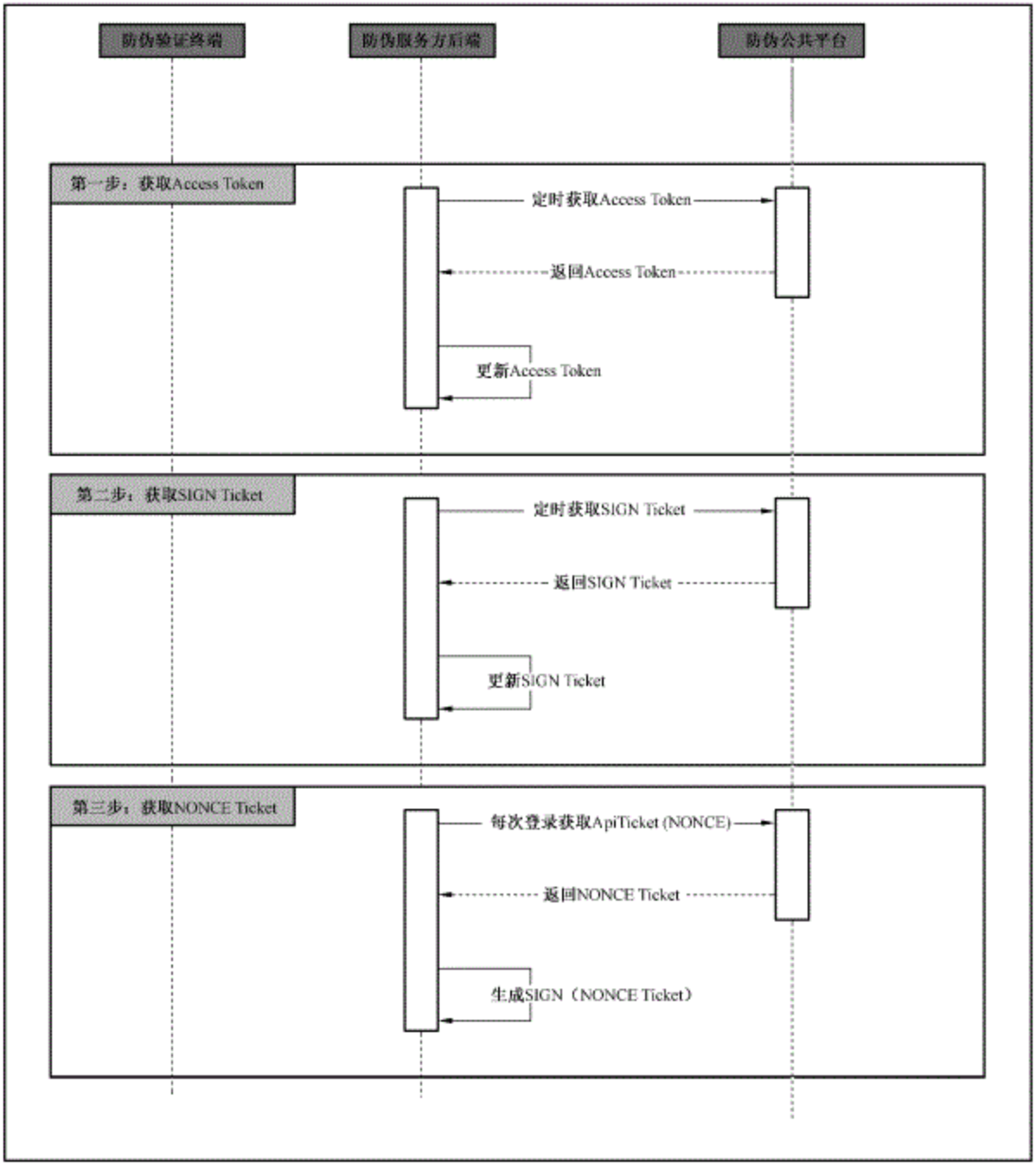

图 A.1 防伪溯源验证接口对接实现流程

附 录 B
（资料性附录）
验证接口反馈数据示例

B.1 反馈数据信息

```
{
    "message": "验证通过：XXXXXXX",// 可用于消费者阅读的文字
    "code": 200,
    "hash": 2432343243243,
    "data": {
        "codeContent": "查询的二维码",
        "codeTime": "查询时间",
        "codeCount": "查询次数",
        "codeType": "防伪技术名称"
    }
}
```

B.2 反馈数据信息说明

B.2.1 message 返回结果

message 返回结果可附带其他任何可被消费者直接阅读的信息。

B.2.2 code 的编码

code 的编码如下：

200 ：验证通过：(请求成功)

201 ：验证完成，码为真，但疑似转移(可能生产批号太久或过去被查询)，消费者根据详细信息确认；

202 ：防伪码不存在；

203 ：防伪码与标识不一致；

204 ：防伪标识不可验证；

205 ：图像质量不满足要求；

100 ：未识别出图片中二维码；请重试；

500：异常(未知的其他情况)；

503：内部服务器错误(含：服务器维护中)；

400：请求参数错误。

B.2.3 hash 值

hash 的值为 data 字段(含花括号，不含 data 后面的冒号)内容的散列码，具体散列算法可由服务端

自行选择，但应在接口文档中写明。客户端收到响应后需要验证散列结果，保证数据传输过程完整性。如验证错误，客户端应该重新查询。

B.2.4 data

data 为返回识别的验证结果信息。

附 录 C
（资料性附录）
必要展示内容字段及说明

必要展示内容字段及对应说明见表 C.1。

表 C.1 必要展示内容字段及说明

序号	字段	说明
1	verification result	验证结果
2	name	产品名称
3	product Factory	生产企业名称
4	brand	品牌
5	norms	产品规格
6	PD	生产日期
7	product Img	产品图片
8	supervision platform	第三方公信监管公共平台
9	support link	投诉链接
10	support hotline	投诉电话

附 录 D
（资料性附录）
扩展展示内容字段及说明

扩展展示内容字段及对应说明见表 D.1。

表 D.1 扩展展示内容字段及说明

序号	字段	说明	备注
1	anti-counterfeiting organization	防伪验证技术服务方	
2	verification frequency	验证次数	
3	verification time	验证时间	
4	verification location	验证地点	
5	customer service call	客服电话号码	
6	short Name	产品简称	
7	classify	分类	唯一
8	explain	产品介绍	
9	place	产品产地	
10	exp	保质期	
11	code	商品条码	
12	address	产品详情页面地址	
13	certificate Img	证书图片	
14	association Id	所属协会社会信用代码	唯一
15	enterprise Id	所属企业社会信用代码	唯一
16	authentication	产品认证	
17	area	投放地区	
18	protect Area	保护范围	
19	create Art	生产工艺	
20	quality	质量特色	
21	contact	联系人	
22	phone	联系电话	
23	addr	联系地址	
24	else Img	其他图片	
25	price	产品价格	
26	dealer	经销商	
27	baile	委托方	
28	E-commerce link	电商销售链接	

附 录 E
（资料性附录）
区块链实施要求

E.1 区块链关键特征

E.1.1 分布式对等

利用对等网络模型，对各参与节点进行组网，并在各对等节点间分配任务和共享资源。网络节点间无需依赖中心节点即可实现信息共享和交换。对等节点既可以是资源、服务和内容的提供者，也可以是获取者。

E.1.2 数据块链式

区块链网络对某一时间段内发生的事务数据进行验证、打包和共识，形成数据区块，为每一个区块与上一个区块按照密码学特征进行有序链接。

E.1.3 不可伪造和防篡改

向区块链写入数据的事务请求需附有发起方私钥签名，该签名随事务请求在网络参与节点间广播并进行验证，实现事务请求不可伪造和防篡改。通过块链式数据结构进一步保证防篡改性。

E.1.4 透明可信

区块链中信息的传递和区块的生成遵循透明的共识规则；每一次事务处理都以特定的形式发送给其他节点，授权节点可以保存与其权限相关的历史记录，保证链上数据的透明性。每一次事务处理和区块生成均可由共识机制授权节点根据既定规则验证其合法性，保证记录结果的可信。

E.1.5 高可靠性

区块链多个节点具有完整的服务能力及全量数据，部分节点的异常或者恶意行为不会影响整体服务的可用性和连续性，以及数据的完整性和真实性。

E.2 存储

存储功能组件提供区块链运行过程中产生的各种类型数据，如账本、交易信息等的写入及查询功能，相关选型包括但不限于关系型数据库、键值对数据库、文件数据库等。

存储功能组件应具备以下功能：

a） 对等网络中，能够被授权全节点部署并使用；

b） 能够高效、安全、稳定地提供数据写入及查询服务。

对于采取分库分表的数据存储方案，存储功能组件还应包括数据的分片及路由处理能力。

E.3 区块链网络搭建

系统管理员的公钥需要被写入在创世区块中。

配置网络的相关参数，如出块时间，区块最大大小、共识机制等。

E.4 上链和查询

将要写入防伪验证及相关数据(或其 hash 值)组装为交易，同步上链，并获得区块及交易 ID。交易中需要包含有：写入操作方、写入时间、写入地点。

交易中可包含相关产品生产和流通环节的特征数据。

根据区块及交易 ID 或相关特征来进行查询，获得在区块链上的存证数据。

E.5 区块链服务提供方

区块链服务提供方应取得国家区块链相关主管机构区块链信息服务的备案。

区块链服务提供方应遵守区块链服务监管方制定并发布的监督管理办法。

参 考 文 献

[1] GB/T 33993—2017 商品二维码