ICS 01.140.40
CCS A 19

中华人民共和国国家标准

GB/T 40949—2021

数字版权保护　可信计数技术规范

Digital rights management—Specification for trusted counting technology

2021-11-26 发布　　2022-06-01 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。

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。

本文件由全国新闻出版标准化技术委员会(SAC/TC 527)归口。

本文件起草单位：中国科学院自动化研究所、北大方正信息产业集团有限公司、中国新闻出版研究院、北京大学、咪咕文化科技有限公司。

本文件主要起草人：张树武、刘杰、黄肖俊、韦玮、梁伟、关虎、王莉、刘颖丽、张倩影、崔晓瑜、俞银燕、顾文扬。

数字版权保护　可信计数技术规范

1　范围

本文件规定了版权资源交易过程中用于可信计数的数据元集合与表示，以及可信性的说明与证实方法。

本文件适用于对数字版权资源的可信交易保护管理。

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 7408—2005　数据元和交换格式　信息交换　日期和时间表示法

3　术语和定义

下列术语和定义适用于本文件。

3.1

数字内容　digital content

以数字形式存在的文本、图像、音频、视频等内容资源。

3.2

版权资源　copyright resources

具有版权信息的数字内容资源。

3.3

可计数性　countability

数字内容的交易数量可被统计的特性。

3.4

可信性　credibility

交易各方都认可和信任的特性。

注：可信性在交易各方利益发生冲突时，保证各方对交易数据和信息相互不可抵赖。

4　缩略语

下列缩略语适用于本文件。

CRI：版权资源标识(Copyright Resources Identification)

5　数据元

5.1　概述

本文件涉及的应用场景和交易流程参见附录A。

本文件涉及的可信计数数据分为销售方生成的权利许可请求基本数据与授权方生成的权利许可基本数据两种类型。权利许可请求基本数据与权利许可基本数据均由基础性数据元、计数性数据元和可信性数据元三部分组成，两者的基础性数据元与计数性数据元相同，可信性数据元不同。

权利许可请求基本数据与权利许可基本数据的示例参见附录 B。

5.2 基础性数据元

描述版权资源的基本信息，数据元见表 1。

表 1 基础性数据元

序号	中文名称	英文标签	类型	必备性	说明
1	版权资源标识	CRI	字符串	是	版权资源的唯一标识符，由授权方提供
2	题名	Title	字符串	是	版权资源的名称
3	版权资源拥有者代码	OwnerID	字符串	是	版权资源的提供者的代码信息，由授权方提供

5.3 计数性数据元

描述版权资源交易的计数信息，数据项见表 2。

表 2 计数性数据元

序号	中文名称	英文标签	类型	必备性	说明
1	交易订单号	TransOrderID	字符串	是	销售系统产生的交易订单号
2	交易数量	TransAmount	整型	是	单个版权资源的交易数量
3	授权附加信息描述	AuthDesc	字符串	否	交易时对该版权资源的授权附加描述信息。包括单一授权和批量授权等，单一授权时可描述购买方信息
4	交易时间	TransTime	日期时间型	是	交易时间信息。符合 GB/T 7408—2005
5	价格	Price	货币型	否	版权资源的价格信息。以人民币（元）为单位
6	授权方代码	AssignorID	字符串	是	版权资源的授权方的代码信息
7	销售方代码	SellerID	字符串	是	版权资源的销售方的代码信息

5.4 可信性数据元

5.4.1 概述

保证数字版权资源交易计数数据可信性的信息。

5.4.2 权利许可请求基本数据的可信性数据元

权利许可请求基本数据的可信性数据元见表 3。

表 3　权利许可请求基本数据的可信性数据元

序号	中文名称	英文标签	类型	必备性	说明
1	交易请求号	TransID	字符串	是	上传交易记录的请求号
2	交易随机数	TransRandom	字符串	是	随机数，用于保证交易数据抵抗重放攻击
3	交易计数器编号	TransCounterID	字符串	是	上传交易记录的计数器编号

5.4.3　权利许可基本数据的可信性数据元

权利许可基本数据的可信性数据元见表 4。

表 4　权利许可基本数据的可信性数据元

序号	中文名称	英文标签	类型	必备性	说明
1	交易请求号	TransID	字符串	是	上传交易记录的请求号，与权利许可请求基本数据交易请求号一致
2	交易随机数	TransRandom	字符串	是	随机数，与权利许可请求基本数据交易随机数一致
3	交易计数器编号	TransCounterID	字符串	是	上传交易记录的计数器编号，与权利许可请求基本数据交易计数器编号一致
4	授权时间	AuthTime	日期时间型	是	授权时间信息。符合 GB/T 7408—2005
5	授权随机数	AuthRandom	字符串	是	随机数，用于保证授权数据抵抗重放攻击
6	授权计数器编号	AuthCounterID	字符串	是	上传授权记录的计数器编号

6　可信性

6.1　完整性

可信计数数据的完整性通过消息摘要技术来保证。

摘要是将计数数据进行指定计算而获得的特殊信息，通过对摘要的验证，检验数据的完整性。

摘要应由两部分组成：

a)　摘要方法：计算摘要信息所使用的算法；

b)　摘要值：通过摘要方法对计数数据计算出来的特殊信息值。

6.2　可验证性

可信计数数据的可验证性通过数字签名来保证。

销售系统和授权系统从第三方可信交易数据管理平台获得私钥，并公开公钥，在提交计数数据时，均对数据的消息摘要进行签名后上传至第三方，并由第三方保存，从而保证交易信息的可验证性。

签名应由两部分组成：

a)　签名方法：计算签名信息所使用的算法；

b)　签名值：通过签名方法对计数数据消息摘要计算出来的特殊信息值。

7 可信性证实方法

数据可信性的验证方法如下：

a) 根据约定的组合方式，将可信计数数据的基础性数据、计数性数据以及可信性数据组合，使用摘要方法对组合信息进行计算得到摘要信息 H1；

b) 使用数据上传者的公钥解密可信计数数据，得到摘要信息 H2；

c) 比较 H1 与 H2，两者一致即表明数据可信，不一致则表明数据不可信。

附 录 A
（资料性）
应用场景和交易流程

A.1 应用场景

版权资源交易应用场景包含购买者、销售方、授权方与第三方可信交易数据管理平台（以下简称管理平台），销售方与授权方向管理平台申请可信计数器。

购买者与销售方进行版权资源交易获取版权资源，从授权方获取资源使用许可。

销售方向授权方发送权利许可请求基本数据，并向管理平台备案。

授权方根据权利许可请求向销售方发送权利许可基本数据，并向管理平台备案。

管理平台收集销售方和授权方的备案数据，保证交易数据的可信性和可计数性。

A.2 交易流程

版权资源交易流程如下。

步骤 1：购买者（终端代理模块）进行版权资源选购。

步骤 2：销售方（交易系统）调用可信计数器生成权利许可请求基本数据，该数据由权利许可请求基本数据和签名数据组成。权利许可请求基本数据元包括基础性数据元（版权资源标识，题名，内容提供者代码）、计数性数据元（交易订单号，交易数量，授权附加信息描述，交易时间，价格，授权方代码，销售方代码）、可信性数据元（交易请求号，交易随机数，交易计数器编号）。数据发送给授权方与管理平台。

步骤 3：授权方（授权系统）调用可信计数器生成权利许可基本数据，该数据由权利许可基本数据和签名数据组成。权利许可基本数据元包括基础性数据元（版权资源标识，题名，内容提供者代码）、计数性数据元（交易订单号，交易数量，授权附加信息描述，交易时间，价格，授权方代码，销售方代码）、可信性数据元（交易请求号，交易随机数，交易计数器编号，授权时间，授权随机数，授权计数器编号）。数据发送给销售方与管理平台。

步骤 4：销售方向购买者提供版权资源，授权方向购买者提供资源使用许可。

步骤 5：交易结束，管理平台确定销售方与授权方数据的匹配情况。

附 录 B
（资料性）
权利许可请求基本数据与权利许可基本数据示例

B.1 权利许可请求基本数据示例

本示例描述权利许可请求基本数据。

```
〈RightRequest〉
    〈CRI〉CRI000A54S1069H02000A9T4120RN280FBHAY0754210850R20210115100238〈/CRI〉
    〈Title〉题名〈/Title〉
    〈OwnerID〉200016578K〈/OwnerID〉
    〈TransOrderID〉TX20200816151349〈/TransOrderID〉
    〈TransAmount〉7〈/TransAmount〉
    〈AuthDesc〉〈/AuthDesc〉
    〈TransTime〉2020-08-16 16:15:13〈/TransTime〉
    〈Price〉15.0〈/Price〉
    〈AssignorID〉AssignorID001131〈/AssignorID〉
    〈SellerID〉SellerID00113802〈/SellerID〉
    〈TransID〉15996000351392〈/TransID〉
    〈TransRandom〉5634086655528265〈/TransRandom〉
    〈TransCounterID〉100026〈/TransCounterID〉
〈/RightRequest〉
```

B.2 权利许可基本数据示例

本示例描述权利许可基本数据。

```
〈RightGrant〉
    〈CRI〉CRI000A54S1069H02000A9T4120RN280FBHAY0754210850R20210115100238〈/CRI〉
    〈Title〉题名〈/Title〉
    〈OwnerID〉200016578K〈/OwnerID〉
    〈TransOrderID〉TX20200816151349〈/TransOrderID〉
    〈TransAmount〉7〈/TransAmount〉
    〈TransTime〉2020-08-16 16:15:13〈/TransTime〉
    〈Price〉15.0〈/Price〉
    〈AssignorID〉AssignorID001131〈/AssignorID〉
    〈SellerID〉SellerID00113802〈/SellerID〉
    〈TransID〉15996000351392〈/TransID〉
    〈TransRandom〉5634086655528265〈/TransRandom〉
    〈TransCounterID〉100026〈/TransCounterID〉
    〈AuthTime〉2020-08-16 16:39:33〈/AuthTime〉
    〈AuthRandom〉8136000816463334〈/AuthRandom〉
    〈AuthCounterID〉100012〈/AuthCounterID〉
〈/RightGrant〉
```