TC260-PG-202602A

网络安全标准实践指南

——网络数据标签标识技术要求

v1.0-202602

全国网络安全标准化技术委员会秘书处

2026 年 2 月

本文档可从以下网址获得：

www. tc260. org. cn/

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国网络安全标准化技术委员会（以下简称“网安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

本文件起草单位：国家计算机网络应急技术处理协调中心、中国电子技术标准化研究院、北京天融信网络安全技术有限公司、中孚信息股份有限公司、北京工业大学、北京邮电大学、国家工业信息安全发展研究中心、中国科学院大学、中国移动通信集团有限公司、联通软件研究院、北京数风科技有限公司、联通数字科技有限公司

本文件主要起草人：陈训逊、李美燕、王晖、赵怀瑾、曲德帅、张露晨、王秀文、王鹏、孙宏跃、胡影、郝春亮、李海东、卓子寒、邢潇、张宇、赵连睿、刘行、高超、周莹、王东滨、公备、辛阳、高明成、冯超、李红飞、吴梦婷、温源、胡迪、秦学鲲、温源、张帅、张腾

声　明

本《实践指南》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。

摘　要

依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规，帮助网络数据处理者使用网络数据标签标识技术提高网络数据安全管理水平，特制定本文件。

本文件提出网络数据标签标识技术的术语和定义、属性格式、生成规则、打标规则、验标规则、日志留存要求、安全防护要求等内容，实现网络数据标签标识技术标准化，可用于帮助网络数据处理者对数据进行标签标识，在此基础上重点对重要数据和个人信息进行分类分级保护，加强数据全周期全过程溯源管理。

目　录

1 范围

本文件提出了网络数据标签标识的属性格式、生成规则、打标规则、验标规则、日志留存要求、安全防护要求等内容。

本文件适用于网络数据处理者开展内部和跨组织数据流动管理。

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 32100 法人和其他组织统一社会信用代码编码规则

GB/T 17969.8 信息技术 对象标识符登记机构操作规程 第 8 部分：通用唯一标识符（UUIDs）的生成及其在对象标识符中的使用

GB/T 20273 信息安全技术 数据库管理系统安全技术要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 31168 信息安全技术 云计算服务安全能力要求

GB/T 38636 信息安全技术 传输层密码协议（TLCP）

GB/T 39205 信息安全技术 轻量级鉴别与访问控制机制

GB/T 42495.1 金融服务 全球法人识别编码 第 1 部分：编码说明

GB/T 43697 数据安全技术 数据分类分级规则

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1 数据对象 data object

以文件或文件集合等方式存储、传输的网络数据。

注：数据对象的数据结构类型可以是结构化、半结构化、非结构化的，包括但不限于数据库、数据表、文本类文件、影音类文件等具体形式。

3.2 数据标签 data label

网络数据处理者为数据对象添加的元数据，通常用于描述数据对象的权属、类别、敏感度等属性。

3.3 数据标识 data label identification

网络数据处理者为数据标签分配的唯一标识符。

3.4 网络数据标签标识技术 labeling and identifying technology for network data

网络数据处理者实现网络数据标签标识的生成、绑定、传输、核验、接收等功能的技术统称。

3.5 静态场景 static application scenarios

网络数据处理者在内部数据管理活动中应用网络数据标签标识技术的场景。

3.6 动态场景 dynamic application scenarios

网络数据处理者在跨组织数据流动管理活动中应用网络数据标签标识技术的场景。

3.7 网络数据打标 network data labeling

网络数据处理者通过技术手段对数据对象和生成的网络数据标签标识进行绑定和传输的处理活动。

注：由于本文件中静态场景不包括数据的传输，动态数据标签标识打标只涉及绑定环节。

3.8 网络数据验标 verifying for network data label

网络数据处理者通过技术手段对收到的数据对象和网络数据标签标识进行核验和接收的处理活动。

注：网络数据验标环节只存在于动态场景下，此处的网络数据标签标识实际上是动态标签标识。

4 缩略语

下列缩略语适用于本文件。

MAC：物理地址（Media Access Control Address）

UUID：通用唯一标识符（Universally Unique Identifier）

JSON：JavaScript 对象表示法（JavaScript Object Notation）

XML：可扩展标记语言 (Extensible Markup Language)

FTP：文件传输协议（File Transfer Protocol）

HTTP：超文本传输协议（Hyper-Text Transfer Protocol）

P2P：对等网络协议（Peer to Peer）

SMTP：简单邮件传输协议（Simple Mail Transfer Protocol）

API：应用程序编程接口（Application Programming Interface）

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

5 网络数据标签标识技术概述

5.1 网络数据标签标识技术架构

网络数据标签标识技术包括网络数据标签标识属性格式和生成、打标、验标等主要技术规范，还包括日志留存及安全防护等技术要求，示意图如图 1 所示。

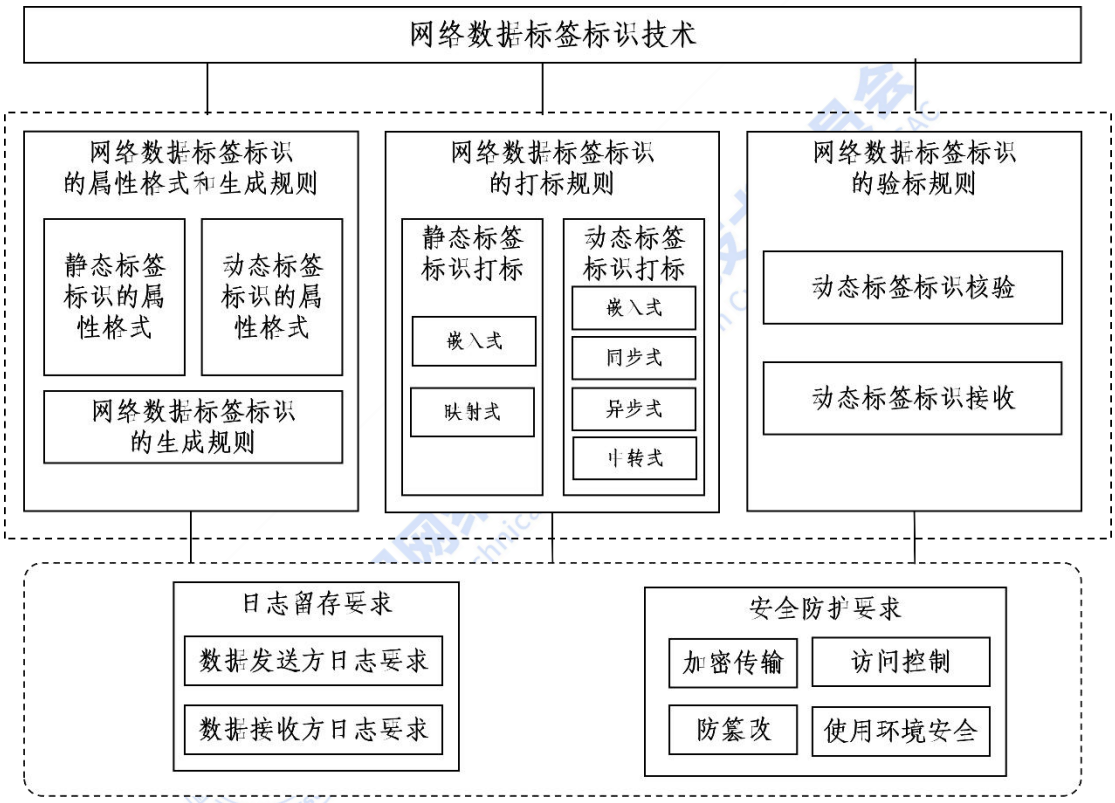

图 1 网络数据标签标识技术架构示意图

5.2 网络数据标签标识技术应用场景

5.2.1 静态场景

网络数据处理者开展内部数据管理时，根据数据存储使用等数据处理活动需要，标记数据的分级、权属特性等静态标签标识信息。

5.2.2 动态场景

网络数据处理者开展跨组织数据流动管理时，根据数据传输、向外提供等数据处理活动需要，标记数据发送方及接收方主体、数据分级、数据规模、时间戳及校验码等动态标签标识信息。典型应用场景包括但不限于本文件附录 A.1 所示网络数据处理者组织间规模化数据流动。

注：规模化数据流动包括单次批量传输和多次单条累积传输等情形。

5.3 网络数据标签标识技术应用流程

5.3.1 网络数据标签标识应用流程概述

网络数据标签标识技术应用应包括网络数据标签标识的生成、绑定、传输、核验、接收、日志留存和安全防护等环节，流程示意如图 2 所示。

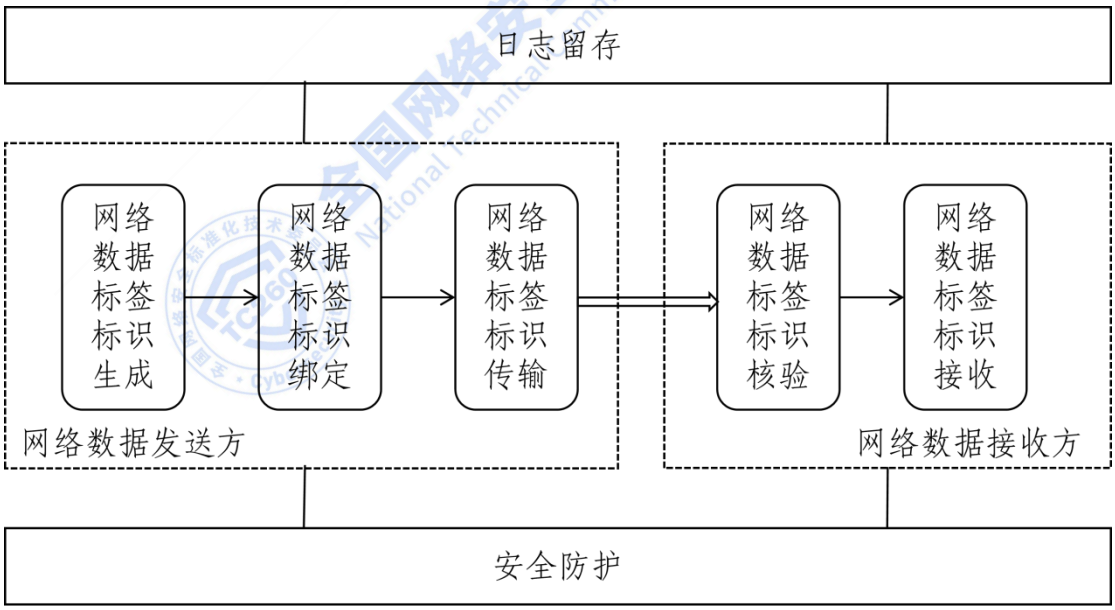

图 2 网络数据标签标识技术应用流程示意图

注：如图 2 所示，一次完整的网络数据标签标识流转过程包括以下环节：某个网络数据处理者甲使用生成的静态标签标识在进行内部数据管理，当准备向另一个网络数据处理者乙进行数据传输时，甲作为数据发送方需要提取静态标签标识相关属性信息，并合并其他属性信息生成动态标签标识，此过程为“网络数据标签标识生成”；接着，数据发送方甲将动态标签标识与数据对象绑定，此过程为“网络数据标签标识绑定”；随后，数据发送方甲将动态标签标识及绑定的

数据对象进行传输，此过程为“网络数据标签标识传输”；然后，数据接收方乙对收到的动态标签标识及数据对象的完整性和关联一致性进行核验，此过程为“网络数据标签标识核验”；最后，数据接收方乙将动态标签标识转换为静态标签标识并存档，此过程为“网络数据标签标识接收”。上述流程中，双方网络数据处理者均需进行日志留存和安全防护，以保障网络数据标签标识的安全性和可用性。数据发送方与数据接收方为不同网络数据处理者在一次数据传输活动中所扮演的不同角色，其角色随数据传输活动的变化而相应转换，例如乙现在向甲传输数据，乙是数据发送方，甲是数据接收方，即开启新的一次网络数据标签标识流转过程。

5.3.2 网络数据打标方式的选择

网络数据处理者根据不同的数据结构类型应采用不同的网络数据打标方式。不同场景下的应用流程示意如附录 A.2 所示。

a) 对于典型的文本类文件等非结构化或者半结构化数据对象，静态场景、动态场景下应采用嵌入式的数据打标方式；

b) 对于典型的数据库等结构化数据对象，静态场景下应采用映射式的数据打标方式，动态场景下根据单次批量或者多次单条两种不同的业务需要应采用同步式、异步式数据打标方式；

c) 对于重要数据处理者、大型网络平台等安全需求较高的情形，宜采用协作平台中转式的数据打标方式。

6 网络数据标签标识的属性格式和生成规则

6.1 静态标签标识的属性格式

6.1.1 数据源主体

数据源主体属性字段表示数据对象采集或加工产生的源头主体，采用 GB 32100 中规定的法人和其他组织统一社会信用代码编码的方式。占位 18 字节。

6.1.2 数据提供方

数据提供方属性字段表示数据对象的直接提供方，采用法人和其

他组织统一社会信用代码编码的方式。占位 18 字节。

6.1.3 数据分级

数据分级属性字段占位 1 个字节，采用二进制编码的方式，按照 GB/T 43697 中相应规则或行业主管部门认定情况对数据对象进行判定是否属于核心数据、重要数据、一般数据、个人信息、敏感个人信息，分别依次对应 8 个比特位的前 5 位，第 6 位表示后续数据是否出境，第 7、8 位作为扩展位留作以后备用，比特位为“1”标识表示“是”，比特位为“0”标识表示 “否” 。

6.1.4 扩展字段

网络数据处理者还可根据实际业务需要增加扩展字段，扩展字段可包含数据分类、安全控制要求、数据传输用途、留存期限、校验/签名等属性内容，本文件不再对扩展字段进行规定。占位 64 字节。

6.1.5 静态标识

静态标识属性字段用于表征静态标签的唯一性标识，可由网络数据处理者按照 GB/T 17969.8 规定的通用唯一标识符（UUID）或其他方式进行编码。占位 16 字节。本字段为可选字段。

6.2 动态标签标识的属性格式

6.2.1 数据源主体

数据源主体属性字段表示数据对象采集或产生的源头主体，采用 GB 32100 中规定的法人和其他组织统一社会信用代码编码的方式。占位 18 字节。

6.2.2 数据发送方

数据发送方属性字段表示本次网络数据传输中数据对象的发送主体，采用 GB 32100 中规定的法人和其他组织统一社会信用代码编码的方式，占位 18 个字节。

6.2.3 数据接收方

数据接收方属性字段表示本次网络数据传输中数据对象的接收主体，对于境内数据接收方采用 GB 32100 中规定的法人和其他组织统一社会信用代码编码的方式，对于境外数据接收方可采用 GB/T 42495.1 中规定的全球法人机构识别编码的前 18 位或其他可唯一标识的编码。占位 18 字节。

注：如 6.1.3 中第 6 位为“0”则此处采用统一社会信用代码的方式，为“1”则此处可采用全球法人机构识别编码的方式。

6.2.4 数据分级

数据分级属性字段占位 1 个字节，采用二进制编码的方式，按照 GB/T 43697 中相应规则或行业主管部门认定情况对数据对象进行判定是否属于核心数据、重要数据、一般数据、个人信息、敏感个人信息，分别依次对应 8 个比特位的前 5 位，第 6 位表示本次传输数据是否出境，第 7、8 位作为扩展位留作以后备用，比特位为“1”标识表示“是”，比特位为“0”标识表示“否”。

6.2.5 数据规模

数据规模属性字段表示本次传输中数据规模，单位为“条”或“字节”。占位 16 字节。其中第一个字节用来标记所使用单位，“0”表

示单位为“条”，“1”表示单位为“字节”；其他字节采用十进制编码表示数值。

注：1 条个人信息，通常指单条可识别特定自然人的数据项，此处特指在一次数据传输中的任意一条个人信息记录，例如企业外发数据表单中包含姓名、电话等多个属性字段的 1 行数据。

6.2.6 时间戳

时间戳属性字段由两部分组成，起始时刻和时间间隔。第一部分标记数据发送传输的起始时刻，精确到毫秒，占位 16 字节。第二部分标记数据传输的时间间隔，描述所生成的动态标签标识的有效期限，精确到秒，占位 8 字节。总占位 24 字节。

注：如果是单条数据传输时间间隔部分设置为空；如果涉及多条数据传输，按照 7.2.3 中注 1 设定。

6.2.7 数据传输校验码

对所传输的数据对象使用密码杂凑算法，杂凑值作为数据传输校验码，用于校验数据对象的完整性，并实现动态标签标识与数据对象的关联。占位 32 字节。

6.2.8 扩展字段

网络数据处理者组织还可根据实际业务需要增加扩展字段，扩展字段可包含数据分类、安全控制要求、数据用途和留存期限等属性内容，本文件不再对扩展字段进行规定。占位 64 字节。

6.2.9 动态标识

动态标识字段用于表征动态标签的唯一性标识，由数据发送方按照 GB/T 17969.8 规定的通用唯一标识符（UUID）进行编码。占位 16 字节。

6.2.10 数字签名

通过非对称加密密码技术，对动态标签标识全部属性字段进行运算，生成的数字签名字段，用于保障动态标签标识的完整性、真实性。占位 64 字节。

6.3 标签标识的生成规则

6.3.1 模板选择

静态场景下应选择适配 6.1 规定的静态标签标识属性格式，动态场景下应选择适配 6.2 规定的动态标签标识属性格式，参考附录 B.1 中属性格式模板示例。

6.3.2 属性获取

静态场景下，网络数据处理者应获取数据对象的数据源主体、数据提供方、数据分级等属性信息。

动态场景下，数据发送方应获取数据对象的数据源主体、数据发送方、数据接收方、数据分级、数据规模、时间戳、数据传输校验码等属性信息，参考附录 B.2 情形 1 示例。其中数据源主体和数据分级属性信息应从静态标签标识中直接获取，其他属性信息应按照网络数据传输活动实际情况设置。

6.3.3 格式选择及标签标识生成

网络数据处理者应选择一种数据格式类型，如：JSON、XML 等，在静态场景和动态场景下分别按照 6.1 或者 6.2 中列出的数据属性格式及顺序生成相应的网络数据标签标识。

6.3.4 安全处理

数据发送方应对动态标签标识的全部属性字段进行数字签名；网络数据处理者可根据自身需要对静态标签标识的全部属性字段进行数字签名。

6.3.5 重新生成

数据对象发生汇聚、加工等处理活动后，如果数据对象相关属性信息发生变化，网络数据处理者应重新获取相应属性信息，重新生成静态标签标识，参考附录 B.2 情形 2 示例。

7 网络数据标签标识的打标规则

7.1 静态标签标识打标

7.1.1 非结构/半结构化数据：嵌入式

网络数据处理者以嵌入式进行静态场景下的数据打标，应符合以下要求：

a）单个文件：非结构化/半结构化数据一般以文件形式存在，应在文件头部或元数据中嵌入静态标签标识。

示例：

诸如 doc、pdf、cvs 等文本类文件，图片、音频、视频等流文件，在文件头部或元数据中增加静态标签标识，也可以使用专用软件工具实现，具体可参考附录 B.3 中图 B.1-图 B.5。

b）文件集合：在对文件进行分级管理基础上，应将同类型文件的静态标签标识以文件的形式与文件集合放入同一个文件夹下。

7.1.2 结构化数据：映射式

结构化数据一般以数据库形式存在。网络数据处理者以映射式进

行结构化数据打标，应符合以下要求：

a）网络数据处理者在不改变现有数据库表结构原则上，宜采用增加静态标签标识映射表的方式实现。

b）网络数据处理者新建数据库系统，可采用直接增加数据源主体、数据提供方、数据分级信息字段的方式实现。

示例：

新增数据分级映射表和数据权属映射表，具体可参考附录 B.3 中图 B.6。

7.2 动态标签标识打标

7.2.1 非结构/半结构化数据：嵌入式

网络数据处理者以嵌入式进行动态场景下非结构/半结构化数据打标，应符合以下要求：

a）数据发送方应将动态标签标识嵌入到非结构/半结构化数据对象进行绑定。

b）数据发送方应将动态标签标识与数据对象合并传输。

示例：

非结构化/半结构化数据一般以文件形式存在，通常有 FTP/HTTP/P2P/SMTP 等多种传输形式，应将动态标签标识与待传输文件或文件集合合并传输。

7.2.2 结构化数据：同步式

网络数据处理者以同步式进行动态场景下结构化数据打标，应符合以下要求：

a) 数据发送方应将生成的动态标签标识自动化封装在应用层协议头部与数据对象进行绑定，随数据对象同步传输。

b) 数据接收方应自动化解析提取识别动态标签标识。

示例：

结构化数据一般采用 API 接口方式进行传输，应用层协议多采用 HTTPS 协议。具体实现方式是在系统统一的 HTTP 调用模块中加入标签绑定逻辑，由程序在数据发送前自动化生成动态标签标识，并写入到 HTTP 协议头部新建的动态标签标识属性中，与数据对象采用 TLS 加密传输，具体可参考附录 B.4 所示。

在数据接收方系统中，需要在 HTTPS 协议处理过程中增加动态标签标识处理功能，用于自动化识别、解析请求头中的动态标签标识。具体实现方式可参考附录 C。

7.2.3 结构化数据：异步式

网络数据处理者以异步式进行动态场景下的结构化数据打标，符合以下要求：

a）数据发送方应在数据对象传输前生成动态标签标识，完成动态标签标识与数据对象的逻辑绑定。

b）数据发送方应按照与数据接收方约定的方式分别传输数据对象及动态标签标识，包括但不限于不同 API 接口传输、不同顺序传输等。

示例：

在异步式数据打标中，数据发送方与数据接收方约定数据对象传输 API 接口与动态标签标识传输接口均采用 HTTPS 协议，例如：数据对象传输接口为 https://xxx/data，动态标签标识传输接口为 https://xxx/label。

c）数据发送方应通过接口功能，实现动态标签标识生成、网络数据打标流程。

d）对于频繁多次传输结构类型相同的单条数据，如附录 A.2 销售服务场景，宜对批量数据进行统一数据打标，通过设定时间周期或设定计数器两种方式实现，时间周期和计数器的设定可根据实际需要由数据发送方和接收方约定适当的粒度。

示例：

设定时间周期模式（数据传输完成后再传输数据标签）。先设定标签生成周期（如 1 天即 86400 秒，则在数据标签时间戳字段中的时间间隔设置为“00086400”）；从该周期内发送第一条数据的起始时间开始算起（在数据标签时间戳字段中的起始时间设置为该时刻），统计在已设定标签生成周期内向同一个应用场景下的同一个数据接收方发送的数据条数（在数据标签数据规模字段设置为该数量）；设置最后一条数据的杂凑值作为数据标签传输校验字段；当该时间周期内的最后一条数据传输完毕后再发送数据标签。

设定计数器模式（数据传输前传输数据标签）。先设定计数器，即标签生成累计条数（如 1000 条，即 1000 条数据累计生成一个数据标签，数据标签数据规模字段设置为“0000000000001000”）；发送时间设置为第一条数据拟发送时间；设置第一条数据的杂凑值作为数据标签传输校验字段。

7.2.4 协作平台：中转式

7.2.4.1 协作平台的适用场景

有下列情形之一的网络数据处理者，宜选择适配协作平台方式，提升网络数据标签标识网络传输的可靠性和安全性：

a）向境外提供重要数据和个人信息的网络数据处理者；

b）重要数据处理者、大型网络平台。

7.2.4.2 动态标签标识存档与转换

数据发送方在发送数据对象前，应将生成的动态标签标识存档至协作平台。

协作平台应将数据发送方发来的动态标签标识映射生成协作平台标识，返回给数据发送方。协作平台标识的生成宜参考 6.2.9 的方法或其他唯一标识方法。

7.2.4.3 协作平台标识传输

数据发送方在发送数据时，应将协作平台标识和相应数据对象发送给数据接收方。

数据发送方应按照本文件7.2.2中规定的同步式或者7.2.3中规定的异步式进行传输。

数据发送方可根据网络环境和传输需求选择适配在应用层、传输层或网络层等位置进行网络数据打标。应用层可参考7.2.2中规定的打标方式，传输层可采用写入TCP扩展位等打标方式，网络层可采用写入IPv6报文扩展头部的打标方式。

7.2.4.4 协作平台标识核验

数据接收方在收到数据对象和相应的协作平台标识后，应向协作平台发起核验请求。

协作平台应根据存档信息对协作平台标识的真实性进行核查，并向数据接收方返回核查结果和动态标签标识。

7.2.4.5 日志留存和安全要求

涉及日志留存，应按照本文件第9章相关要求执行；涉及安全防护，应按照本文件第10章相关安全要求执行。

8 网络数据标签标识的验标规则

8.1 动态标签标识核验

数据接收方应对接收到的动态标签标识进行完整性校验，并与数据对象进行关联一致性核验，最后将核验结果反馈给数据发送方。

8.2 动态标签标识接收

数据接收方核验无误后，应先将动态标签标识转换为静态标签标识，根据接收数据的数据结构类型采用不同的处理方式：

a）对于非结构化/半结构化数据，将动态标签标识中的数据源主体、数据发送方、数据分级等属性信息取出生成静态标签标识，参考非结构化/半结构化数据的静态标签标识打标方式，完成静态标签标识的嵌入式绑定，参考 B.2 情形 1。

b）对于结构化数据将动态标签标识中的数据源主体、数据发送方、数据分级等属性信息取出生成静态标签标识，参考结构化数据的静态标签标识打标方式，在静态标签标识映射表中增加或者修改映射信息。

数据接收方应在完成标签转换后，存储收到的数据对象和生成的静态标签标识，并维护数据对象和相应静态标签标识的关联。

9 日志留存要求

9.1 数据发送方日志要求

数据发送方在动态标签标识生成和网络数据打标环节，应按如下要求记录并保存日志。

a）动态标签标识生成、绑定和传输操作记录，包括但不限于执行者、执行时间、执行方式、执行结果、生成和传输的动态标签标识内容等；

b）数据对象信息，包括但不限于非结构化/半结构化数据文件路径；结构化数据库名、表名、字段名、用户名、操作指令等；传输的数据对象存证信息，包括数据采样和相应动态标签标识。数据采样留存比例应基于统计学中的平方根采样原则。

c）数据源主体信息，包括但不限于组织机构统一社会信用代码、组织机构名称等。

d）数据接收方信息，包括但不限于组织机构统一社会信用代码、组织机构名称等。

e）数据对象用途信息，包括但不限于数据交易、委托处理等。

9.2 数据接收方日志要求

数据接收方在网络数据验标环节，应按如下要求记录并保存日志。

a）动态标签标识接收及核验操作记录，包括但不限于执行者、执行时间、执行方式、执行结果、接收的动态标签标识内容等。

b）数据对象信息，包括但不限于非结构化/半结构化数据文件存储路径；结构化数据存储的库名、表名、字段名、用户名、操作指令等；接收的数据对象存证信息，包括数据留样和相应的动态标签标识。数据采样留存比例应基于统计学中的平方根采样原则。

c）数据源主体信息，包括但不限于组织机构统一社会信用代码、组织机构名称等。

d）数据发送方信息，包括但不限于组织机构统一社会信用代码、组织机构名称等。

e）数据对象用途信息，包括但不限于数据交易、委托处理等。

10 安全防护要求

10.1 加密传输

数据发送方应采用诸如 HTTPS 的安全传输协议对网络数据标签

标识进行加密传输，可参考 GB/T 38636 等。

10.2 访问控制

数据接收方应采用访问控制等技术对在内部存储的网络数据标签标识及相关日志记录进行安全保护，确保仅授权人员可访问相关信息，可参考 GB/T 39205 等。

10.3 防篡改

数据发送方和接收方应采用密码技术对网络数据标签标识的完整性进行校验，对网络数据标签标识及相应数据对象的关联一致性进行验证。

10.4 使用环境安全

在网络数据标签标识的生成、传输、存储、使用及核验等环境，应符合国家网络安全等级保护、数据库管理安全、云计算服务安全等要求，可参考 GB/T 22239、GB/T 20273 和 GB/T 31168 等。

附 录 A

（资料性）

网络数据标签标识技术应用示例

A.1 网络数据标签标识技术典型应用场景参考示例

A.1.1 生产制造场景

网络数据处理者同上游供应商、零部件制造商、外包加工厂、下游合作方等主体共享数据，如汽车制造企业在总装环节需获取发动机、传感器、电子控制单元等零部件的质量与生产批次数据，以确保整车一致性；电子产品制造企业需从代工厂获取生产线良品率、温湿度控制及关键工序日志等信息，用于产品质量追溯与生产过程优化。

A.1.2 销售服务场景

网络数据处理者与经销商、服务商、物流企业之间传输订单数据、客户数据等，如生活服务平台将用户预订机票酒店信息同步至合作方航空公司、酒店，电商平台将用户支付信息、订单信息同步至金融机构、第三方合作商家，网约车平台将乘客订单数据同步至第三方运力公司等，但不包括向个人用户侧的数据传输。

A.1.3 流通交易场景

网络数据处理者在数据要素流通和社会治理领域，需要和第三方机构共享统计分析、业务监测或监管数据，以及企业在数据交易平台上进行数据产品流通等。

A.1.4 日常办公场景

网络数据处理者在日常办公中跨组织的文件流转，主要涉及通过电子邮件和社交软件等方式向企业外部传递文件，诸如办公文档文件和图片影音文件等。

A.2 网络数据标签标识技术应用流程图

a）静态标签标识的生成和打标流程见图 A.1 所示。

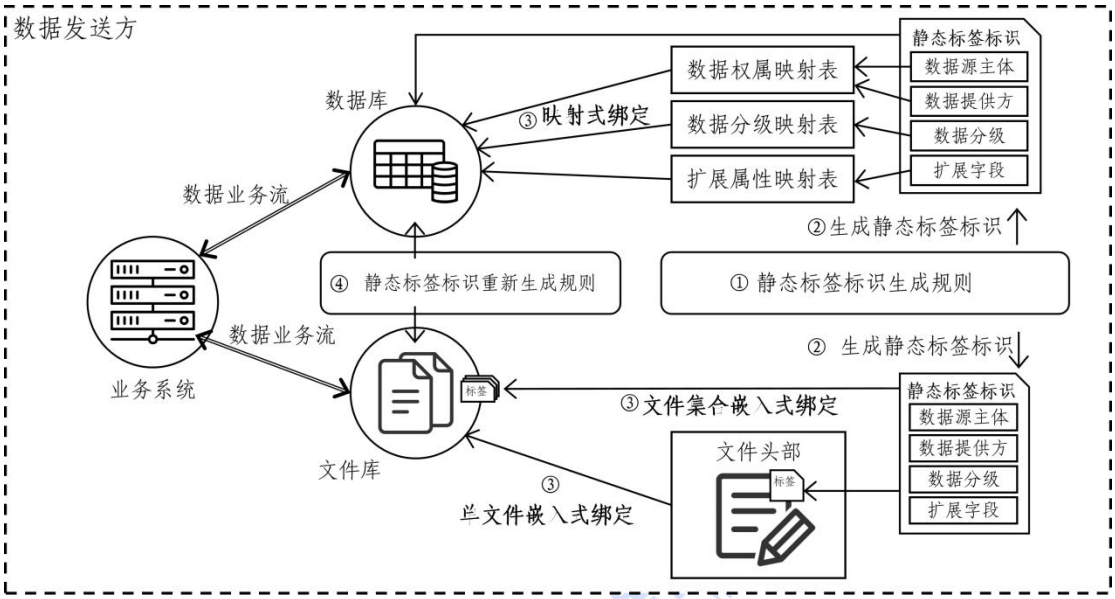

图 A.1 静态标签标识的生成和打标流程示意图

b）动态标签标识的生成和打标流程见图 A.2 所示。

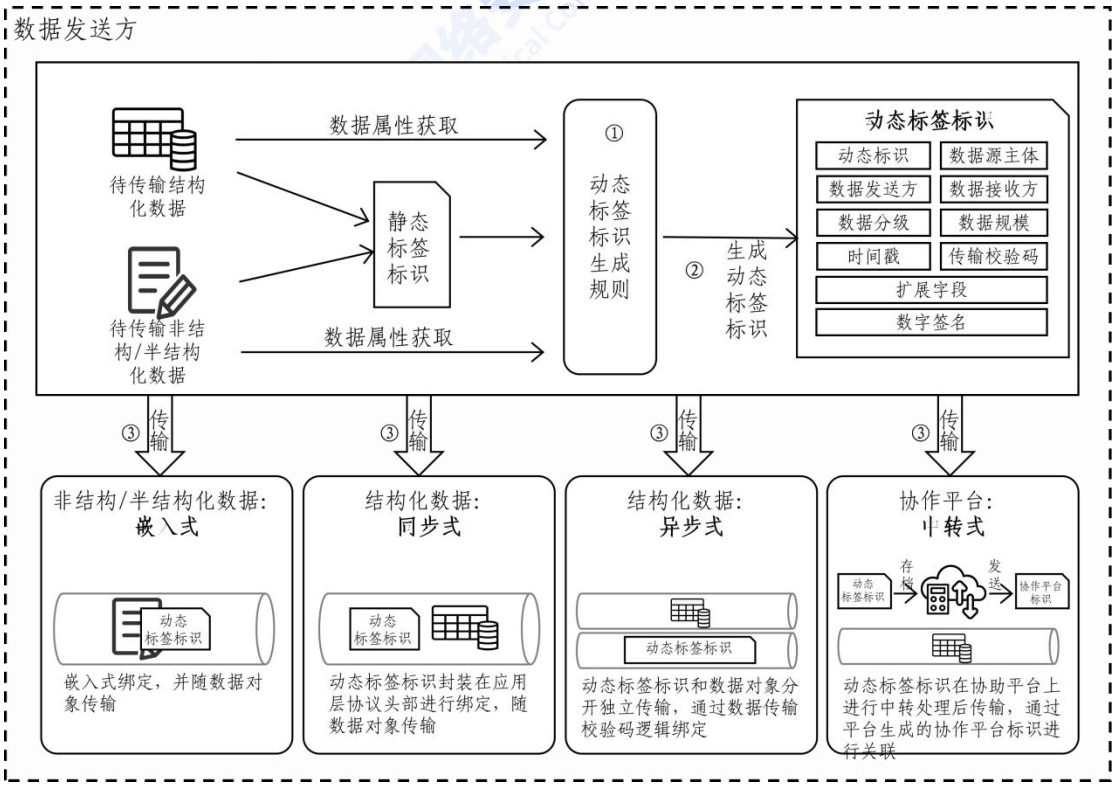

图 A.2 动态标签标识的生成和打标流程示意图

c）动态标签标识的验标流程见图 A.3 所示。

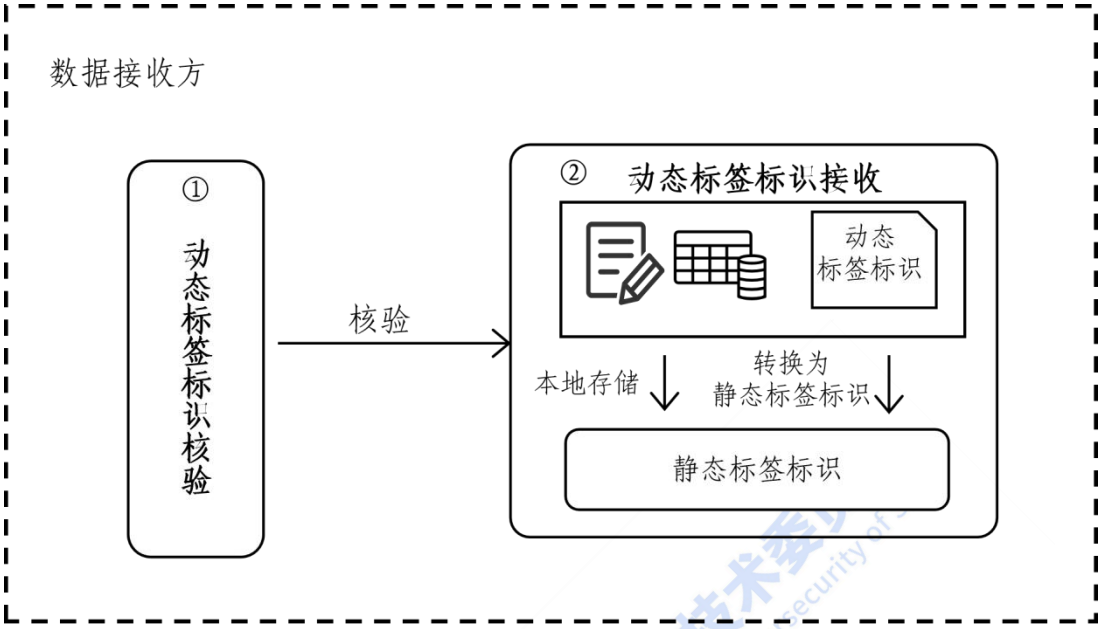

图 A.3 动态标签标识的验标流程示意图

d）引入协作平台后，动态标签标识的生成、打标和验标流程见图 A.4 所示。

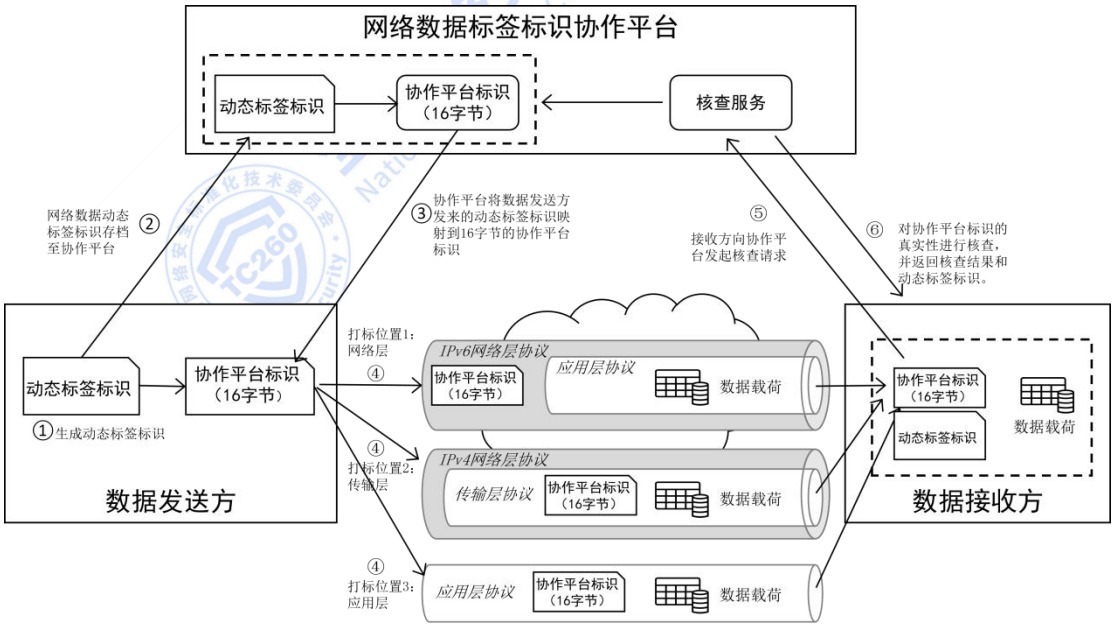

图 A.4 协作平台动态标签标识的生成、打标和验标流程示意图

附 录 B

（资料性）

网络数据标签标识格式示例

B.1 网络数据标签标识属性格式模板示例

B.1.1 静态标签标识属性格式模板示例

静态标签标识属性格式模板示例见表 B.1 所示，丙公司存储的数据是从乙公司（统一社会信用代码为 914405123456358117）处获得的，并且数据源主体是甲公司（统一社会信用代码为 12165432117800056Q），则编码后的静态标签标识是“12165432117800056Q914405123456358117000111 00”。若乙公司存储的数据是自有数据，即数据发送方和数据源主体均是乙公司，则编码后的静态标签标识是“914405123456358117914405123456358117000111 00”。

表 B.1 静态标签标识属性格式模板示例

字段	长度（B）	示例数据	说明
数据源主体	18	12165432117800056Q	丙公司所存储数据对象的源头是甲公司。
数据提供方	18	914405123456358117	该数据对象由乙公司直接提供给丙公司。
数据分级	1	00011100	该数据对象既是个人信息、又是敏感个人信息、且未来可能出境、但不属于重要数据
扩展字段	64	——	可由企业根据需要自定义。

静态标识	16	550e8400e29b41d4a716446655440000	UUID 通常表示为 32 个十六进制字符。

B.1.2 动态标签标识属性格式模板示例

动态场景下网络数据标签标识模板示例见表 B.2 所示，甲公司将内部存储的自有数据传输给乙公司，则编码后的动态标签标识是“550e8400e29b41d4a71644665544000012165432117800056Q12165432117800056Q914405123456358117000111000000000000000128202510150830150000000864001ab21d8355cfa17f8e61194831e81a8f22bec8c728fefb747ed035eb5082aa2bf596d18be77035b0bb9ef6abf23ae9e81f2df3178bedd56d64220dc72c6883a61b92ddc4c167e22956e5af32ce65bf4c05f9d6d96aa82c41ace0aa28acba9234”。

表 B. 2 动态标签标识属性格式模板示例

字段	长度 (B)	示例数据	说明
数据源主体	18	12165432117800056Q	本次数据流转过程中的数据源主体是甲。
数据发送方	18	12165432117800056Q	本次数据流转过程中的数据发送方是甲。
数据接收方	18	914405123456358117	本次数据流转过程中的数据接收方是乙。
数据分级	1	00011100	与静态标签标识中的分级属性一致。
数据规模	16	0000000000000128	数据规模是 128 条。
时间戳	24	202510150830150000000	表示 2025 年 10 月 15 日上午 8 点 30 分

		86400	15 秒开始传输，时间间隔为 1 天。
数据传输校验码	32	1ab21d8355cfa17f8e61194831e81a8f22bec8c728fefb747ed035eb5082aa2b	密码杂凑算法应按照国家密码管理的相关规定进行选择和使用。
扩展字段	64	——	可由企业根据需要自定义。
动态标识	16	550e8400e29b41d4a716446655440000	UUID 通常表示为 32 个十六进制字符。
数字签名	64	f596d18be77035b0bb9ef6abf23ae9e81f2df3178bedd56d64220dc72c6883a61b92ddc4c167e22956e5af32ce65bf4c05f9d6d96aa82c41ace0aa28acba9234	对动态标签标识的全部属性字段进行数字签名

B.2 数据属性获取与变更示例

情形 1：甲收到来自乙的自有数据，直接转发给丙。甲收到的动态标签标识中权属信息相关属性为：“数据源主体是乙，数据发送方是乙，数据接收方是甲”；甲将收到的动态标签标识转换为静态标签标识，权属信息相关属性更新为：“数据源主体是乙，数据提供方是乙”；转发给丙，需要生成新的动态标签标识，权属信息相关属性更新为：“数据源主体是乙，数据发送方是甲，数据接收方是丙”。

情形 2：甲收到来自乙的自有数据，经过甲加工后，转发给丙。更新后的数据标签中权属信息相关属性为：“数据源主体是甲，数据发送方是甲，数据接收方是丙”。因加工处理活动，数据主体已由乙变成了甲。

B.3 静态标签标识示例

嵌入式静态标签标识示例见图 B.1 所示，采用 JSON 语言描述。

下面就不同场景下的应用进行示例：

```
"static_label": {
        "subject_identifier": "12165432117800056Q",          //数据源主体
        "sender_identifier": "12165432117800056Q",           //数据发送方
        "classification_grading_info": "00011100"            //数据分级
        "extension": ""                                      //扩展字段
    }
```

图 B.1 嵌入式静态标签标识示例

a）pdf 文件元数据嵌入静态标签标识示例见图 B.2 所示。

```
<?xpacket begin="    " id="W5M0MpCehiHzreSzNTczkc9d"?>
<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 4.4.0-Exiv2">
  <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
    <rdf:Description rdf:about=""
      xmlns:cls="http://ns.example.org/classification/1.0/">
        <cls:static_label>12165432117800056Q12165432117800056Q00011
        100</cls:static_label>
    </rdf:Description>
  </rdf:RDF>
</x:xmpmeta>
<?xpacket end="w"?>
```

图 B.2 pdf 文件元数据嵌入静态标签标识示例

b）图片文件元数据嵌入静态标签标识示例见图 B.3 所示。

```
compression:JPEG
thumbnail_offset:205926
thumbnail_length:15963
XMP toolkit:XMP Core 4.4.0-Exiv2
Static_Label:{"static_label":"12165432117800056Q12165432117800056Q00
        011100"}
profile_CMM_type:
profile_version:0.0.1
profile_class:display_device_profile
```

图 B.3 图片文件元数据嵌入静态标签标识示例

c）音频文件元数据嵌入静态标签标识示例见图 B.4 所示。

```
major_brand:M4A
minor_version:512
```

compatible_brand:isom ios4
Static_Label:{"static_label":"12165432117800056Q12165432117800056Q00
011100"}
encoder:Lavc59.27.101
duration:00:04:55,58
start:0.025057
bitrate:128kb/s
stream#0:0
audio:mp3,44100Hz,stereo,s16p,128kb/s

图 B.4　音频文件元数据嵌入静态标签标识示例

d）视频文件元数据嵌入静态标签标识示例见图 B.5 所示。

major_brand:isom
minor_version:512
compatible_brand:isom iso3 avc1 mp43
Static_Label:{"static_label":"12165432117800056Q12165432117800056Q00
011100"}
endcoder:Lavf59.27.100

图 B.5 视频文件元数据嵌入静态标签标识示例

e）数据库新增静态标签标识映射表示例见图 B.6 所示。

数据库1

	编号	姓名	银行卡号	性别
表1	0	张三	6228 3321 2234 0987	男
	1	李四	3228 3463 5234 9980	男
	2	王五	4238 5402 6234 8984	女
	3	赵六	3428 3433 5245 9983	女

	编号	姓名	身份证号	住址
表2	0	张三	123456789012123456	北京市海淀区中山路09号
	1	李四	323456789012654321	北京市朝阳区上海路03号
	2	王五	323456789018765432	北京市顺义区南京路08号
	3	赵六	423456789987654983	北京市海淀区河北路

	表名	字段名	分级映射	静态数据分级标识
数据分级映射表	表1	姓名	个人信息	00010000
		银行卡号	敏感个人信息	00011000
		性别	个人信息	00010000
	表2	姓名	个人信息	00010000
		身份证号	敏感个人信息	00011000
		住址	个人信息	00010000

	表名	编号	数据源主体标识	数据发送方标识
数据权属映射表	表1	0	121654321178000560	121654321178000560
		1	121654321178000560	121654321178000560
		2	121654321178000560	121654321178000560
		3	121654321178000560	121654321178000560
	表2	0	121654321178000560	121654321178000560
		1	121654321178000560	121654321178000560
		2	121654321178000560	121654321178000560
		3	121654321178000560	121654321178000560

	表名	编号	扩展属性
扩展属性映射表	表1	0	type:a,class:b.....
		1	type:a,class:b.....
		2	type:a,class:b.....
		3	type:a,class:b.....
	表2	0	type:a,class:b.....
		1	type:a,class:b.....
		2	type:a,class:b.....
		3	type:a,class:b.....

图 B.6 数据库新增静态标签标识映射表示例

B.4 动态标签标识示例

同步式的动态标签标识示例如图 B.7 所示。

```
"dynamic_label": {
        "subject_identifier": "12165432117800056Q",          //数据源主体
        "sender_identifier": "12165432117800056Q",           //数据发送方
        "receiver_identifier": "914405123456358117",         //数据接收方
        "classification_grading_info": "00011100",           //数据分级
        "data_scale": "0000000000000128",                    //数据规模
        "timestamp": "20251015083015000-00086400",           //时间戳
        "data_transmission_check":
   "1ab21d8355cfa17f8e61194831e81a8f22bec8c728fefb747ed035eb5082aa2b"
                                                             //数据传输校验码
        "extension": ""                                      //扩展字段
        "label_id":"550e8400e29b41d4a716446655440000",       //动态标识
        "signature": "f596d18be77035b0bb9ef6abf23ae9e8
                      1f2df3178bedd56d64220dc72c6883a6
                      1b92ddc4c167e22956e5af32ce65bf4c
                      05f9d6d96aa82c41ace0aa28acba9234"      //数字签名
    }
```

图 B. 7 同步式的动态标签标识示例

下面以 HTTPS 为例描述如何进行同步式数据打标，如图 B.8 所示。图中描述数据发送方与数据接收方之间通过 API+HTTPS 进行数据传输的过程，包括 HTTPS 请求报文和响应报文内容：请求报文中，请求的方法为 GET，headers 为请求头（数据发送方和接收方的标识、请求体格式为 JSON）；响应报文中，headers 为响应头（动态标签标识为 dynamic_label、响应体格式为 JSON），body 为数据内容（包含响应的数据内容 data 和元数据 metadata）。

图 B.8 动态场景下采用 API 技术接口和 HTTPS 传输协议的数据打标示例

附 录 C

（资料性）

同步式打标的实现方式示例

本附录在 7.2.2 的示例基础上，给出了网络数据标签标识同步式打标的几种实现方式。

C.1 反向代理实现方式

适用于业务系统使用了 Nginx 等反向代理的情况。此方式在应用层通过反向代理服务器对 HTTP（S）流量进行中转处理，利用其头部操作指令（如 add_header, proxy_set_header）实现标签标识的注入，实现同步式打标。

C.2 API 网关实现方式

在系统入口处通过 API 网关组件对所有进出流量进行统一处理，基于路由规则和过滤（或“插件”）机制实现标签标识的添加与转发。通过配置 API 网关的策略或编写简单的处理脚本，可为特定路由的请求或响应添加标签标识，实现同步式打标。

C.3 应用层中间件实现方式

通过在业务应用程序内部嵌入统一的数据标签标识处理模块。基于拦截器或过滤器机制，在 HTTP 响应返回前，由中间件组件将数据标签标识嵌入到 HTTP 头部，实现同步式打标。

C.4 应用系统实现方式

通过直接修改业务系统服务端每个 API 接口的代码，在生成响应

时，通过调用相应编程语言或框架提供的设置 HTTP 头部的函数（例如，在 Java 中可使用 response.setHeader 方法），将数据标签标识嵌入到 HTTP 响应头部，实现同步式打标。