公开

中国团体标准

T/BEA 20003-2025

基于区块链的智能电能表计量数据溯源规范

Specification for smart electricity meter measurement data traceability based on blockchain

2025－11－17 发布　　2025－11－20 实施

北京电子仪器行业协会　　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这些专利的责任。

本文件由北京市标准化研究院提出。

本文件由北京电子仪器行业协会归口。

本文件起草单位：一能充电科技（深圳）股份有限公司、北京市标准化研究院 、北京节能环保中心、南方电网数字电网集团有限公司、华北电力大学、国网区块链科技（北京）有限公司、中国科学院数学与系统科学研究院、中国农业银行河北雄安分行、上海电力交易中心有限公司、大唐水电科学技术研究院有限公司、中国中元国际工程有限公司、上海市数字证书认证中心有限公司、国网北京市电力公司、内蒙古电力（集团）有限责任公司、华北电力大学技术转移转化中心、国网冀北电力有限公司、国网湖北省电力有限公司经济技术研究院、浙江电力交易中心有限公司、北京信息科技大学、北京东方计量测试研究所、国网北京市电力公司通州供电公司、国网山东省电力公司营销服务中心（计量中心）、国网北京市电力公司门头沟供电公司、国网黑龙江省电力有限公司营销服务中心、国网山西省电力有限公司营销服务中心、深圳供电局有限公司、广西电网有限责任公司、贵州电网有限责任公司、海南电网有限责任公司、国网江苏省电力有限公司营销服务中心、国网冀北电力有限公司营销服务中心、国网重庆市电力公司营销服务中心、国网河北省电力有限公司信息通信分公司、国网河北省电力有限公司营销服务中心、国网山东省电力公司聊城供电公司、北京京能科技有限公司、国网北京市电力公司朝阳供电公司、国网北京市电力公司信息通信分公司、国网北京市电力公司昌平供电公司、深圳职业技术大学、深检集团（浙江）质量技术服务有限公司、宁波送变电建设有限公司永耀科技分公司。

本文件主要起草人：周锡忠、贾月芹、李文峰、曾璐琨、李晓丹、孙干、杨剑、彭巍巍、胡桂明、徐向东、王超、王清、王平欣、程昱舒、杨芾藜、苏宇、黄志伟、王伟贤、余涛、陈春逸、沈阅、李豪、胡常昊、郑永康、劳大实、徐祺、朱亮亮、刘书涵、郑尚卓、杨景旭、周政雷、杨婧、钟磊、张志远、张靓、何莹、陈林、李彬、李闯、郭庆雷、张学森、薛文昊、张君石、李雪蓉、王宏盛、杨光、刘茜、王泽黎、刘惠颖、文茹馨、程含渺、赵志宇、孟超、葛利宏、郭琦、路石俊、奥韦、康毅、雷庆生、王雅文、王怡聪、朱振良、吴雁南、张琪、马麟、姜振宇、崔凯、赵思翔、王宏宇、王玉贞、王少影、卢艳艳、李骥、李万信、张荣浩、王小享、王成祖、鲍敏忠、徐颖天、顾炜炜、杨劲松、李刚、郭智慧、胡兴婷、解博钧、李卫萍、姜维、申莉莉、张家乐、尹晓博、刘知羽、李志华、周杰、张丽萍、窦冲、辛红金、陈思。

基于区块链的智能电能表计量数据溯源规范

1 范围

本文件确立了基于区块链的智能电能表计量数据溯源的技术架构，规定了数据上链及溯源流程，以及 DID 注册、VC 生成与上链、数据溯源与验证等环节的技术要求。

本文件适用于基于区块链的智能电能表计量数据的溯源。

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 25069 信息安全技术 术语

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32918.2 信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分：数字签名算法

GB/T 42752 区块链和分布式记账技术 参考架构

GB/T 43572 区块链和分布式记账技术 术语

GB/T 43580 区块链和分布式记账技术 存证通用服务指南

DL/T 645 多功能电能表通信协议

DL/T 698.45 电能信息采集与管理系统 第 4-5 部分：通信协议—面向对象的数据交换协议

T/BEA 20001-2025 基于分布式数字身份（DID）的电碳计量智能电能表数据格式规范

T/BEA 20002-2025 基于区块链的电碳计量智能电能表与采集主站的数据交互规范

3 术语和定义

GB/T 25069、GB/T 43572、T/BEA 20001-2025、T/BEA 20002-2025 界定的以及下列术语和定义适用于本文件。

3.1

电能信息采集终端 electrical energy data acquisition terminal

负责各信息采集点的电能信息的采集、数据管理、数据传输以及执行或转发主站下发的控制命令的设备，按应用场所可分为厂站采集终端、专变采集终端、公变采集终端和低压集中抄表终端(包括低压集中器、低压采集器)等类型。

[来源：DL/T 698.1-2021，3.2]

3.2

可验证凭证 verifiable credential；VC

一种由发行方签发的、包含关于主体身份或属性声明的防篡改数据单元。

3.3

默克尔证明 Merkle proof

用于证明某个数据项属于特定默克尔树的路径信息，包含从该数据项到根节点的兄弟节点杂凑值序列。

3.4

锚定 anchoring

将某个数据、哈希值或状态记录到区块链上，利用区块链的不可篡改性和时间戳能力，为该数据提供一个可验证、可追溯、不可否认的存在性证明。

3.5

数据溯源 data provenance

数据在整个生存周期内（从产生、传播到消亡）的演变信息和演变处理内容的记录。
[来源：GB/T 34945-2017，2.1]

4 缩略语

下列缩略语适用于本文件。
API：应用程序编程接口（Application Programming Interface）
DID：分布式标识符（Distributed Identifier）

5 技术架构

5.1 概述

技术架构构建了从数据采集前端到区块链可信存储再到应用验证的链路闭环，实现智能电能表计量数据从源头到应用的全流程可信交互。技术架构见图 1。

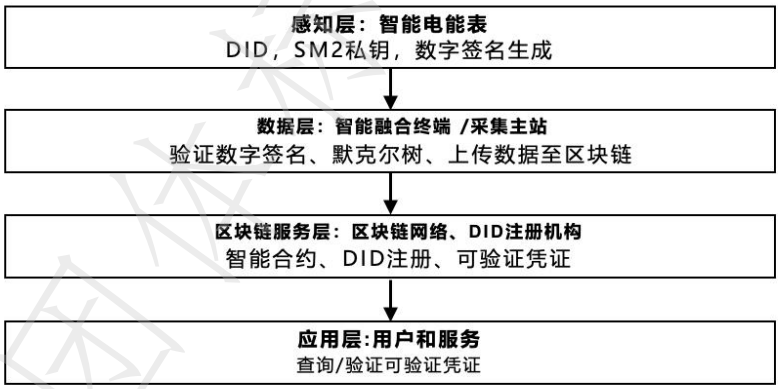

图 1 智能电能表计量数据区块链溯源技术架构

各层级之间通过标准化接口进行数据交互，具体如下：

a) 感知层与数据层：应采用 DL/T 645 或 DL/T 698.45 规定的通信协议进行数据交换，应符合 T/BEA 20002 规定的交互机制与协议；
b) 数据层与区块链服务层：通过区块链开放 API 交互，将数据上传至区块链网络存证；
c) 应用层与区块链服务层：通过 API 获取存证信息和验证结果。

5.2 感知层

感知层识别、采集环境或设备的状态和数据。感知层设备主要包括智能电能表。每台智能电能表应分配标识该设备身份的唯一 DID。智能电能表应内置安全模块存储私钥。

5.3 数据层

数据层具备以下功能：

a） 汇聚、处理和转发来自智能电能表的数据；
b） 对智能电能表生成的签名数据进行初步校验；
c） 将校验后的数据打包生成 VC，并通过区块链接口提交至区块链网络进行存证；
d） 承担智能电能表 DID 的辅助注册和管理功能。

注：在电力系统中，数据层由电能信息采集终端或采集主站实现。

5.4 服务层

服务层由区块链网络和分布式身份注册机构组成，为上层应用提供数据存证、溯源验证、身份管理等核心服务。区块链的基本架构应符合 GB/T 42752 的相关规定。

a） 区块链网络是由多个节点组成的联盟链或私有链，通过运行智能合约实现计量数据的上链存证和身份管理功能。区块链网络包括记账节点、共识节点等，该网络维护一个共享的分布式账本，用于存储智能电能表读数数据的杂凑值与相关凭证。所有计量数据存证交易在链上按照时间顺序打包成区块，并通过默克尔树关联形成可追溯的链式结构，为数据不可篡改性和可验证性提供技术基础。
b） DID 注册机构是指提供 DID 管理服务的系统，负责 DID 的注册、更新、撤销及解析，可由区块链网络中的特定节点或智能合约承担。DID 注册机构支持每个智能电能表、代理节点等获得唯一的 DID，并将对应公钥写入链上 DID 文档。新加入系统的设备或参与方，应通过 DID 注册机构注册身份，获取可信的分布式标识。

5.5 应用层

应用层包括电力消费者、售电公司、碳交易平台等终端用户以及提供数据服务的应用系统。终端用户可通过 API 查询智能电能表的链上计量数据存证，获取由智能电能表签发的 VC，并将其用于电费结算、能源交易、碳核查等用途。数据使用方（如交易平台）作为验证方，可从链上获取由特定智能电能表 DID 签发的 VC，验证其签名和完整性后用于业务办理。

6 数据上链及溯源流程

基于区块链的智能电能表计量数据上链及溯源包括三个部分，分别是 DID 注册、VC 生成与上链、数据溯源与验证，见图 2。

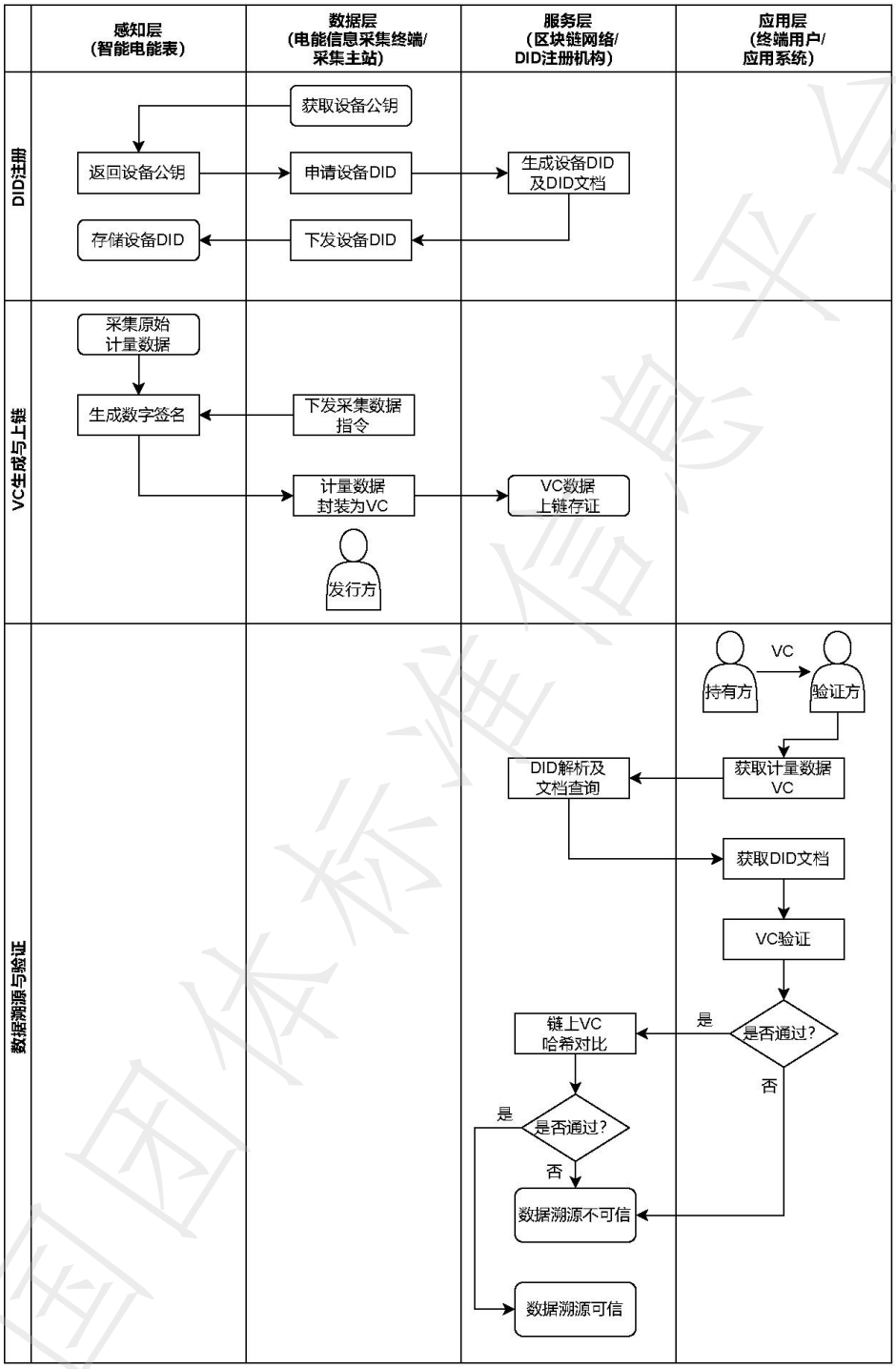

图 2　基于区块链的智能电能表计量数据上链及溯源流程

7　DID 注册

7.1　DID 格式

每个参与主体均应具有唯一的 DID。该标识符格式参照《Recommendation Decentralized Identifiers (DIDs) v1.0》的 DID 数据模型设计。智能电能表的 DID 应在其出厂校准接入区块链网络时生成。生成方式宜采用去中心化方法，例如基于电能表序列号或公钥杂凑生成。系统应提供 DID 注册智能合约接口，新设备的 DID 应由授权机构（如供电公司）在区块链上注册，写入对应的 DID 文档。

7.2 DID 文档

DID 文档宜采用 JSON-LD 格式，参照《JSON-LD 1.1 A JSON-based Serialization for Linked Data》设计，内容包括 DID 主体的公钥和服务信息等元数据，示例见附录 A。对于智能电能表，DID 文档至少应包括以下内容：

a) DID：智能电能表的 DID，唯一对应该智能电能表；
b) VerificationMethod：智能电能表用于签名的公钥列表，每个公钥应包括唯一标识（如键 ID）、类型（如 SM2）以及公钥值。智能电能表出厂时应由制造商为其生成密钥对，并将公钥写入 DID 文档；
c) Authentication：用于认证智能电能表身份的验证方法，应引用 verificationMethod 中的公钥。例如，可指定智能电能表 DID 下的主私钥对应的公钥为认证密钥；
d) Service（可选）：服务端点列表，可用于描述该主体提供的服务。例如智能电能表可以定义一个数据服务端点，指向其电能信息采集终端或数据缓存的地址，服务类型可定义为 MeterReadingService。

7.3 DID 注册流程

DID 注册流程如下：

a) 智能电能表所属单位（如供电公司或设备厂商）生成智能电能表的密钥对；
b) 调用区块链上的 DID 注册合约，将智能电能表 DID 及其公钥注册到区块链上；
c) 注册完成后，参与方可通过 DID 在链上查询到对应的公钥，用于后续验证智能电能表签名数据以及 VC。

8 VC 生成与上链

8.1 数据签名

8.1.1 杂凑值计算

应使用符合GB/T 32905规定的SM3杂凑算法对原始计量数据执行运算并生成256位杂凑值。若原始数据为 JSON 格式，应先按键名字典序排序，再序列化为UTF-8字节串后进行计算，保持不同实现环境下结果一致。该杂凑值作为数字签名的消息摘要。

8.1.2 数字签名

应使用符合GB/T 32918.2的SM2签名算法对上述摘要进行签名。签名使用与智能电能表DID关联的私钥。

8.1.3 签名附加信息

在签名过程中应引入附加信息，例如将智能电能表的 DID、读数时间标签一并参与杂凑或在签名时引入随机数。引入附加信息时，应保持记录的完整性，并在凭证或存证数据结构中显式标注。

8.1.4 签名消息格式

应明确字段及算法标识，提高互操作性。签名消息格式宜参照JSON Web Signature (JWS)或JSON Web Token (JWT)的要求进行封装。

8.2 VC 封装

8.2.1 通用要求

智能电能表产生的计量数据应封装为VC。VC的数据模型参照《Verifiable Credentials Data Model v2.0》的相关要求。智能电能表及其代理节点或智能电能表所有方作为发行方针对某次计量读数生成VC，VC中应包括相关声明和密码学证明,示例见附录A。

8.2.2 数据模型

智能电能表读数VC的数据模型宜通过JSON-LD定义，保持字段类型和格式一致，兼容不同区块链平台的数据交换格式，可扩展字段并支持语义互操作。

8.2.3 签发

智能电能表代理节点或智能电能表所有方在计量周期结束或达到触发条件时，应签发读数VC，签名算法应符合GB/T 32918.2的规定。

8.3 上链存证

8.3.1 通用要求

智能电能表的电能信息采集终端或者采集主站应将新签发的VC进行上链存证。存证过程应符合GB/T 43580的相关规定。

8.3.2 上链模式

8.3.2.1 边缘代理上链模式

智能电能表通过本地通信网络向电能信息采集终端传输计量数据。电能信息采集终端对数据进行汇聚和签名，并作为区块链客户端或节点，将数据摘要及证明信息上传区块链。智能电能表与电能信息采集终端之间的数据传输若在过程中发现异常（如数据校验失败、签名验证未通过），应中止上链并触发告警。

8.3.2.2 主站上链模式

智能电能表向采集主站传输数据。采集主站完成校验和存储后，作为区块链客户端或节点，将数据或摘要写入区块链上。采集主站作为数据发行方，以其自身 DID 签名并提交存证。

8.3.2.3 混合上链模式

在同一系统中，可同时存在边缘代理上链和主站上链两种方式，形成混合上链模式。混合上链模式下的互操作要求包括：

a) 采集主站应能获取电能信息采集终端上链数据，并归档入本地数据库；
b) 已由电能信息采集终端上链的数据，采集主站无需重复上链，但可将其链上杂凑值纳入主站记录，以统一对外查询接口；
c) 验证方在查询时，应能获得一致的数据结构和验证流程，不因模式差异而影响验证结果。

8.3.3 存证方式

计量数据的链上存证可采用以下三种方式：

a) 直接交易存证：每条计量数据 VC 生成一笔区块链交易，关键数据作为交易内容保存；
b) 批量存证：多条计量数据杂凑值组成默克尔树，仅记录根值上链，单条数据可通过默克尔证明验证；
c) 日志事件存证：利用区块链事件日志功能，将数据锚定信息写入链上日志，适用于高频场景。

8.3.4 区块结构关系

在直接交易模式下，每条读数作为独立交易写入区块，在批量模式下，每个批次生成一条交易，内容包括一个默克尔根。两种模式最终均纳入区块链的默克尔树结构，并随区块杂凑值形成整体账本。

8.3.5 隐私与安全

电能数据的明文不应直接写入区块链，宜将其杂凑值或加密索引上链。业务数据（如汇总电量）应进行脱敏处理或以区间汇总形式存储。区块链平台应支持国家密码算法（如SM2、SM3），并符合GB/T 32918.2和GB/T 32905的规定。

9 数据溯源与验证

验证方在核实智能电能表计量数据时，应按以下步骤进行。

a) 获取 VC：验证方应获取待验证的智能电能表读数 VC。获取方式包括通过 VC ID 从区块链查询并获取完整 VC 内容，或者通过持有方直接获取完整 VC 内容。若仅有 VC 摘要，系统应提供获取原始 VC 的方法。
b) 验证 DID：解析 VC 得到发行方的 DID 后，验证方应调用区块链 DID 解析接口，检索该 DID 的最新 DID 文档，确认其状态有效，并提取公钥。
c) 验证签名：验证方应使用 DID 文档中的公钥，对 VC 签名进行验证。具体方法为：对 VC 除签名部分外的内容计算杂凑值，并使用公钥验证该杂凑值与签名值的一致性，其中杂凑算法应符合 GB/T 32905 的规定，签名验证算法应符合 GB/T 32918.2 的规定。若验证失败，该 VC 不应被接受。
d) 一致性比对：验证方应将 VC 的杂凑值与区块链存储的杂凑值比对，或通过默克尔树证明 VC 包含于默克尔根中。在直接存证模式下，应比对 VC 杂凑值与链上杂凑值一致性，在批量模式下，应使用存证的默克尔证明和区块链上的默克尔根进行验证。
e) 状态与时效：验证方应检查 VC 的状态与有效期。状态管理可采用状态列表或撤销列表形式。验证方可通过 VC ID 查询相关状态，若 VC 已被撤销或超过有效期，则视为无效。
f) 业务采信：经验证后，若 VC 真实性、完整性与时效性均符合要求，验证方可将其用于业务场景，例如电费结算、电量交易或碳排放核算。验证结果（包括验证时间、验证方 DID、验证结论等）可写入区块链，供后续审计追溯。

附 录 A
（资料性）
智能电能表 DID 文档与 VC 示例

A.1 智能电能表 DID 文档示例

A.1.1 DID 文档实例

假设有一台智能电能表，其 DID 为 did:energy:01XHJQ8Z72PA3，该智能电能表拥有一把 SM2 公钥用于签名数据，公钥值为 BGrVX...k1Y=。此外，该智能电能表提供一个数据查询服务接口。其 DID 文档如下：

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:energy:01XHJQ8Z72PA3",
  "verificationMethod": [{
    "id": "did:energy:01XHJQ8Z72PA3#key-1",
    "type": "SM2VerificationKey2025",
    "controller": "did:energy:01XHJQ8Z72PA3",
    "publicKeyMultibase": "BGrVX...k1Y="
  }],
  "authentication": [
    "did:energy:01XHJQ8Z72PA3#key-1"
  ],
  "service": [{
    "id": "did:energy:01XHJQ8Z72PA3#MeterService",
    "type": "MeterReadingService",
    "serviceEndpoint": "https://utility.example.com/meters/01XHJQ8Z72PA3"
  }]
}
```

A.1.2 示例说明

上述 JSON 中，publicKeyMultibase 字段省略了一部分中间值，以“...”表示。实际应为 SM2 公钥的完整值。该 DID 文档表明：

——此智能电能表以 DID 标识 did:energy:01XHJQ8Z72PA3 注册；

——拥有一个 SM2 公钥（标识为#key-1），由智能电能表自身控制，可用于验证其签名；

——该密钥同时被指定为认证用途（authentication）；

——提供了一个类型为“MeterReadingService”的服务，其端点为电力公司提供的查询接口统一资源定位符（URL），其参与方可通过此服务获取该智能电能表的数据（需适当的授权）。

A.2 智能电能表计量数据 VC 示例

A.2.1 计量数据 VC 示例

以下示例 VC 由上述智能电能表（发行方）签发，表示该表在 2025-08-26 09:55 采集的电量读数：

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://example.com/energy-meter/v1"
  ],
  "id": "urn:uuid:7f54a419-8c2c-4ef2-afd3-2032d8f5e9a5",
  "type": ["VerifiableCredential", "MeterReadingCredential"],
```

```
  "issuer": "did:energy:01XHJQ8Z72PA3",
  "issuanceDate": "2025-08-26T09:55:05Z",
  "credentialSubject": {
    "id": "did:energy:01XHJQ8Z72PA3",
    "meterReading": 1234.56,
    "unit": "kWh",
    "timestamp": "2025-08-26T09:55:00Z"
  },
  "proof": {
    "type": "SM2Signature2025",
    "created": "2025-08-26T09:55:05Z",
    "verificationMethod": "did:energy:01XHJQ8Z72PA3#key-1",
    "signatureValue": "MEUCIFb6...Zr1t"
  }
}
```


A.2.2 示例说明

该数据 VC 说明：

——此 VC 采用两个上下文：一个是基本 VC 上下文，另一个 energy-meter/v1 假定定义了 MeterReadingCredential 类型以及 meterReading、unit 等字段；

——id 是 VC 的唯一识别码，具有全局唯一性；

——type 表明它是 MeterReadingCredential；

——issuer 是智能电能表 DID；

——issuanceDate 为签发时间，略晚于读数采集时间几秒钟；

——credentialSubject 包含智能电能表自身的 DID 和读数值 1234.56 kWh，及对应采集时间戳；

——proof 部分表示使用 SM2 签名，verificationMethod 指向智能电能表 DID 文档中的公钥#key-1。signatureValue 为签名值（这里为长度为约 88 字符的 Base64 字符串，实际截断表示），验证方可用智能电能表公钥验证此签名与上述内容匹配，确认读数的真实性。

当该 VC 提交上链存证时，链上可只保存其杂凑值。例如计算上述凭证 JSON 的 SM3 杂凑值得到 3ACB...F9D（假设值），区块链存储 credentialId = urn:uuid:...映射到 hash = 3ACB...F9D。验证方日后拿到凭证原文，再计算杂凑值比对即可验证链上记录一致性。

以上示例展示了符合本文件的数据格式。实际系统中可根据业务需求和安全策略扩充字段或上下文。

参 考 文 献

[1] GB/T 34945-2017 信息技术 数据溯源描述模型

[2] DL/T 698.1-2021 电能信息采集与管理系统 第1部分：总则

[3] RFC 7515. JSON Web Signature(JWS)[EB/OL]. https://www.rfc-editor.org/rfc/rfc7515.html.

[4] RFC 7519. JSON Web Token (JWT)[EB/OL]. https://www.rfc-editor.org/rfc/rfc7519.html.

[5] W3C. Decentralized Identifiers (DIDs) v1.0[EB/OL]. https://www.w3.org/TR/did-1.0/.

[6] W3C. JSON-LD 1.1 A JSON-based Serialization for Linked Data[EB/OL]. https://www.w3.org/TR/json-ld11/.

[7] W3C. Verifiable Credentials Data Model v2.0[EB/OL]. https://www.w3.org/TR/vc-data-model-2.0/.