



中华人民共和国国家标准

GB/T XXXXX—XXXX

安全与韧性 产品和文档的真实性、完整性和可信性 建立互信与互操作性框架指南

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines to establish a framework for trust and interoperability

(ISO 22385:2023, MOD)

草案版次选择

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布

XXXX - XX - XX 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 II

引言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 方案治理文件 2

5 适用于 ESEDS 方案参与者的建议 2

6 组织措施 3

7 技术措施 3

8 内部方案资源 3

9 目录 3

附录 A（资料性） ESEDS 示例 1

附录 B（资料性） 每个目录的可见数字印章方案示例 6

参考文献 9

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。

本文件修改采用ISO 22385:2023《安全和韧性 产品和文档的真实性、完整性和可信性 建立互信与互操作性框架指南》。

本文件与ISO 22385:2023的技术差异及其原因如下：

- 更改了“范围”，删除了适用于“实体”“产品”的范围，以适用于我国国情（见第1章）；
- 更改了“列表”，增加了各项措施技术要求的详细描述（见第7章）。

本文件由全国公共安全基础标准化技术委员会（SAC/TC 351）提出并归口。

本文件起草单位：中国标准化院、北京金谷远见科技集团有限公司、内蒙古自治区质量和标准化研究院、中国防伪行业协会、中检集团天帷网络安全技术(合肥)有限公司、东方蓝天钛金科技有限公司、北京信息科技大学、南浔区市场监督管理局、随州市标准化与行政许可技术审查中心、天津市标准化研究院、责扬天下(北京)管理顾问有限公司、天津晟龙科技发展有限公司、北京东方计量测试研究所、中国计量测试协会、北京市科学技术研究院。

本文件主要起草人：周倩、毕力格、张金芳、郭德华、罗隼、闫亚坤、殷格非、严明、涂明扬、孙国华、谷玉海、王宇航、孙彩英、秦挺鑫、毕晓宇、叶季青、管竹笋、刘浩、屈莹、黄帅、张王磊、王皖、石雅婷、朱振良、杨倚天、苟龙龙、白鑫。

引 言

在数字世界中建立信任、实现互操作性和相互协作至关重要。为减轻因伪造电子文档、软件和服务造成的损失，有必要考虑数字层面的安全防护机制。

当供应链中的任何人，包括分销商、独立经纪人、执法机构和终端客户，都可以使用电子签名编码数据集（ESEDs）方案来访问产品或文档的安全本地或远程描述时，这些方案就可以用于防止伪造。应用于各种特定和单个项目或统一资源标识符（URI）的通用且唯一的数据完整性检查机制有助于及早发现假冒品。

本文件事关电子签名编码数据集方案，旨在通过描述必要的可信环境，实现可靠和安全的（软件、服务等）认证和可追溯性流程。这将有助于在产品和文档价值链中通过真实标注和监控机制实现信任服务的互操作性。

本文件所提出的电子签名编码数据集案完全自愿实施，独立于其他认证和跟踪追溯系统。

使用电子签名编码数据集访问来自本地或远程来源的可信数据，可为终端用户和执法人代理机构提供发现伪造品的有效工具，从而降低接触伪造品和文件的风险。

电子签名编码数据集使用电子签名功能对数据的完整性进行验证，并识别/验证安装了ESEDs的产品或文件的制造商/发行人的身份。验证过程既可在线上或离线状态下完成，具体方式则需借助由已签署的使用场景描述文件（“列表”）所支持的各项功能。

电子签名编码数据集可以作为一组电子数据和/或作为机器可读代码（MRC）显示和读取。

这些指导原则的实施可以使不同市场部门和市场参与者共享相同的全球ESEDs方案架构和语义、角色定义以及相关流程。通过这种方式，可以实现部门互操作性和全球范围内的交互操作。

打击供应链中的电子文档、软件和服务的欺诈行为是一项关键挑战。欺诈问题严重影响分包商、合作伙伴和供应商。与此同时，越来越多的国家和国际的法规要求全面的“背靠背责任”，如美国、欧盟的《产品责任指令》以及欧盟的《通用数据保护条例》（GDPR）。

通过使用电子签名编码数据集建立信任与互操作性将有助于实现“背靠背责任”的一致性。这将有助于正确理解不同市场部门针对某一特定产品、子产品、软件和服务在不同市场领域中的UID。可实现对文件、软件或服务进行可互操作的在线和/或离线识别和真伪查验。

这意味着来自不同市场部门的所有参与者需对完整的电子签名编码数据集方案、其管理模式及其文件层次和结构有着相同的理解。

图1中的流程图总结了电子签名编码数据集全局方案。

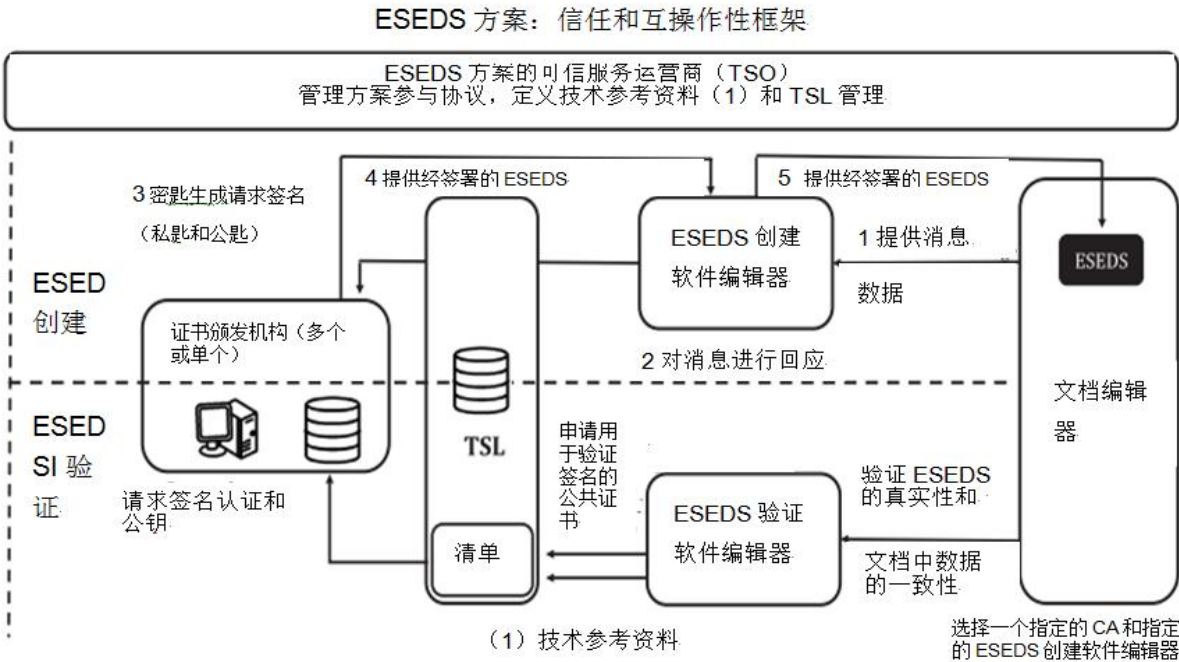


图 1 电子签名编码数据集方案

本文件包含以下要素，可用于设计一个可靠可信的电子签名编码数据集：

- 方案的基础文件（见第 4 章）；
- 适用于该方案参与者的建议（见第 5 章）；
- 组织措施（见第 6 章）；
- 技术措施（见第 7 章）；
- 内部方案资源（见第 8 章）；
- 目录（见第 9 章）。

这些条款是ESEDS方案管理模式的基本要素。每一条条款均由一份或数份文件构成，这些文件描述了不同ESEDS计划参与者须履行的强制性内容。

ESEDS方案的所有基本要素如图2中的层次结构所示。

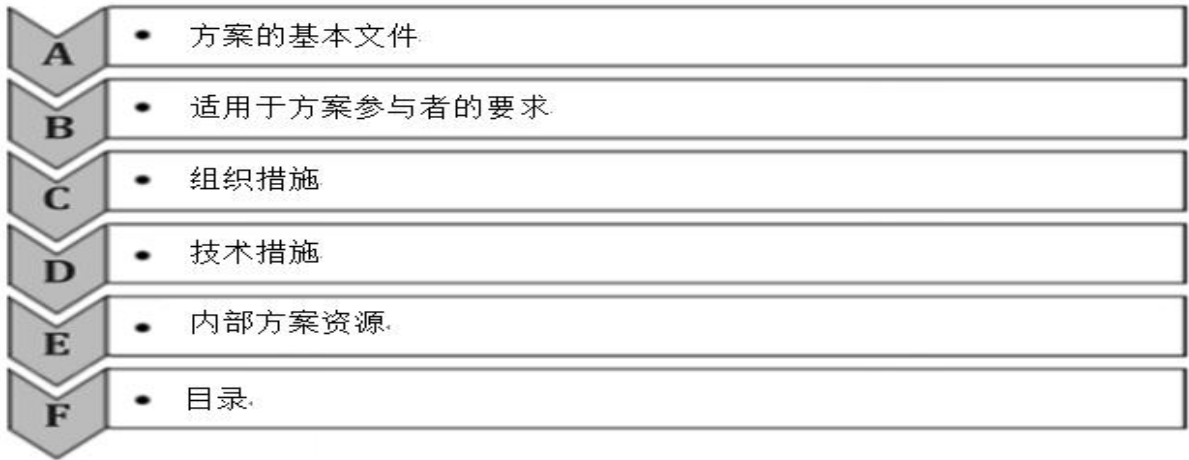


图 2 电子签名编码数据集基本要素

与国际民用航空组织（ICAO）模式（仅涉及跨国母/子分级认证机构）相比，本文件提出的ESEDs模式可供多个独立认证机构（CA）应用。因此，本文件提出的信任环境组织允许分级CA模式（如ICAO）和基于多部门CA的部门、国家或国际模式进行合作。基于这种方法，只要使用公共数据结构，就可以开发出对任何用例都不加限制的通用读取器应用程序（可信入口点，TEP）。若遵循本文件的规则和原则，则可以将电子签名编码数据集系统视为一个潜在的全局信任环境。最终，独立可信服务运营方（TSO）信任网络之间的互操作性可以通过使用相同的通用数据结构，基于适当的标准和规范，并通过互认其各自的电子签名编码数据集方案来实现。

本文件适用于安全和可互操作识别系统的开发人员和用户。本文件面向所有行业开放，不受技术类型限制，不会妨害现有的识别、跟踪和追溯以及身份认证系统，但能够在这些系统之间引入交互机制。

本文件是包括ISO 22380、ISO 22381、ISO 22382、ISO 22383和ISO 22384在内的系列标准之一。

安全与韧性

产品和文档的真实性、完整性和可信性

建立互信与互操作性框架指南

1 范围

本文件通过使用对象识别技术确立了一个可信的信息处理和通信环境框架，该框架可以保护相关电子文档、软件和服务在整个生命周期内供应链的完整性，减少产品欺诈和假冒伪劣商品。

本文件提供了建立框架的指南，该框架通过安全可靠的电子签名编码数据集（ESEDs）方案为多参与者应用程序提供信任和互操作指导，也适用于多部门环境。

本文件不会妨碍现有的追溯、识别和身份认证系统，能够通过引入ESEDs方案来支持这些系统之间的互操作。

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 44483 安全与韧性 术语

3 术语和定义

GB/T 44483界定的以及下列术语和定义适用于本文件。

3.1

电子签名编码数据集 ESEDs electronically signed encoded data set ESEDs

包含报头、有效负载、签名和可选辅助数据块的结构化数据集。

注1：有效负载类型和颁发机构标识包含在报头中。

注2：ESEDs通常可以表示为机器可读代码（3.3）。

3.2

信任服务运营方 TSO trust service operator TSO

是完整的电子签名编码数据集（ESEDs）（3.1）方案的唯一所有者的法律实体，履行以下三个角色职能：

- 管理信任服务列表；
- 管理列表；
- 提供 ESEDs 方案的运行管理规则。

3.3

机器可读代码 MRC machine-readable code MRC

图形符号或电子设备，或二者的组合，包含一组可由数据采集系统理解的符号或字母。

注：MRC的示例包括但不限于2D条形码和无线射频识别（RFID）标签。

3.4

可信入口点 TEP trusted entry point TEP

由可信服务运营方（3.2）提供和/或认证的方法，其支持格式化响应功能（RFF）并且对能够无歧义地解决任何唯一标识符（UID）的附加对象识别和认证系统（OIAS）开放。

3.5

信任服务列表 TSL trust service list TSL

包含有关可信服务运营方(3.2)、信用服务提供方(TSPs)以及经授权可签发证书以电子方式签署编码数据集(3.2)的TSP证书颁发机构(CA)的合规信息列表。

注1：ETSI TS 119 612规定了符合要求的信任服务列表的相关描述。

注2：信任服务列表可使用可信服务运营方（3.2）规定的可扩展标记语言（XML）进行扩展。

3.6

信用服务提供方 TSP trust service providerTSP

参与电子签名编码数据集（ESEDs）（3.1）方案并能够提供以下多种功能或信用服务的法律实体：

- 电子证书；
- 电子签名；
- 时间戳；
- 与 ESEDs 方案要求相关的任何其他信用服务。

3.7

背靠背责任 back-to-back liability

将责任从承包商完全转移给分包商。

3.8

列表 manifest

用例列表，包含XML格式信息的外部资源，这些信息与每个单独的电子签名编码数据集（3.1）用例、其数据模式、验证策略和可选扩展有关。

4 方案管理文件

4.1 基础方案管理文件由信任服务运营方创建。

4.2 方案管理文件作为电子签名编码数据集方案管理模式的参考文件应被所有参与者接受。

4.3 所有参与者均应同意受方案管理约束。

4.4 方案管理文件提供了主要原则，用于描述参与电子签名编码数据集方案所需的成员协议中应包含和列出的核心要素。

4.5 方案管理文件的主要目的是定义电子签名编码数据集方案中参与者的角色、责任和义务。

5 适用于电子签名编码数据集方案参与者的技术规范

信任服务运营方定义电子签名编码数据集方案应包含对方案参与者有影响的五个技术规范，具体如下：

- 技术规范 1：明确规定电子签名编码数据集方案的信用服务供应商如何确保方案参与者对电子签名编码数据集方案建立信心的技术措施；
- 技术规范 2：明确规定信用服务提供商如何保证在电子签名编码数据集方案中其服务水平一致性的技术措施；
- 技术规范 3：明确规定电子签名编码数据集创建系统如何确保互操作性的技术措施；
- 技术规范 4：明确规定电子签名编码数据集验证软件如何确保互操作性的技术措施；
- 技术规范 5：明确规定文件发布者如何确保互操作性的技术措施。

6 组织措施

6.1 信任服务运营方定义电子签名编码数据集方案应包括一份专门的文件，描述所有行为者和参与者所遵循的生命周期管理过程。

6.2 电子签名编码数据集方案的所有参与者均应使用该文件。

7 技术措施

7.1 信任服务运营方定义电子签名编码数据集方案可以遵循其他标准或规范，其中包括描述电子签名编码数据集或类似数据结构需使用的数据组织的技术措施。

示例：ISO/IEC 20248:2022 或 AFNOR XP Z42-105:2019，对文件或物体携带的数据进行认证、验证和获取的电子存储规范。

7.2 附录 A 给出了电子签名编码数据集的使用案例。

8 内部方案资源

8.1 信任服务运营方定义电子签名编码数据集方案应包括以下内部方案资源：

- 一个可公开访问且机器可读的信任服务列表，目标是确保信用服务提供方的列表是公开的；
- 一份提供必要输入和机制的列表，该方案可以适用于不同的信用服务、数据展示和离线验证。

8.2 这两个内部方案资源应在两个单独的技术规范中进行描述。

9 列表

9.1 信任服务运营方定义电子签名编码数据集方案应具有四个不同的列表，这四个列表对全局电子签名编码数据集方案的互操作性至关重要。目录应包括以下信息：

- 列表编号 1：**参与者列表**，用于核验参与方的方案准入协议有效性与主体资质；
- 列表编号 2：**方案认定的合格信任供应方的列表**，用于核验信用服务提供方的服务资质与授权有效性；
- 列表编号 3：**电子签名编码数据集软件创建编辑器列表**，用于核验创建工具的合规性与授权有效性；
- 列表编号 4：**电子签名编码数据集软件验证编辑器列表**，用于核验验证工具的合规性与授权有效性。

9.2 附录 B 给出了每个目录的可见数字印章（VDS）方案的一个示例。

附录 A
(资料性)
ESEDs 示例

A.1 概述

A.1.1 电子签名编码数据集的一个常见示例是可见数字印章。可见数字印章包括在二维条形码中嵌入物体的基本信息，嵌入物体可以是文件、安全标签或安全牌，具体可参见第A.2条中给出的半导体电子签名编码数据集示例。这些信息由数据哈希表的电子签名锁定，这保证了签发组织的身份和嵌入物体的完整性。二维码的数据由与放置在电子印章证书X.509中的公钥相对应的私钥进行电子签名。这种非对称加密方式允许供应链的所有参与者使用签名签发组织的公钥来控制签名。电子证书的交付受信任服务运营方控制，信任服务运营方验证可见数字印章签发组织是否有权签发该文件。签名由生成电子印章的信用服务提供方执行。任何实体可通过TEP验证签名。如果数据的签名是正确的，这表明相关数据（并且仅限此类数据）是正确的。此类数据可以用作新应用程序或另一个用例的可信输入数据。

A.1.2 第A.2至A.7条中给出了用例示例。

A.2 使用案例：半导体电子签名编码数据集

A.2.1 图A.1显示了某个半导体电子签名编码数据集的结构。

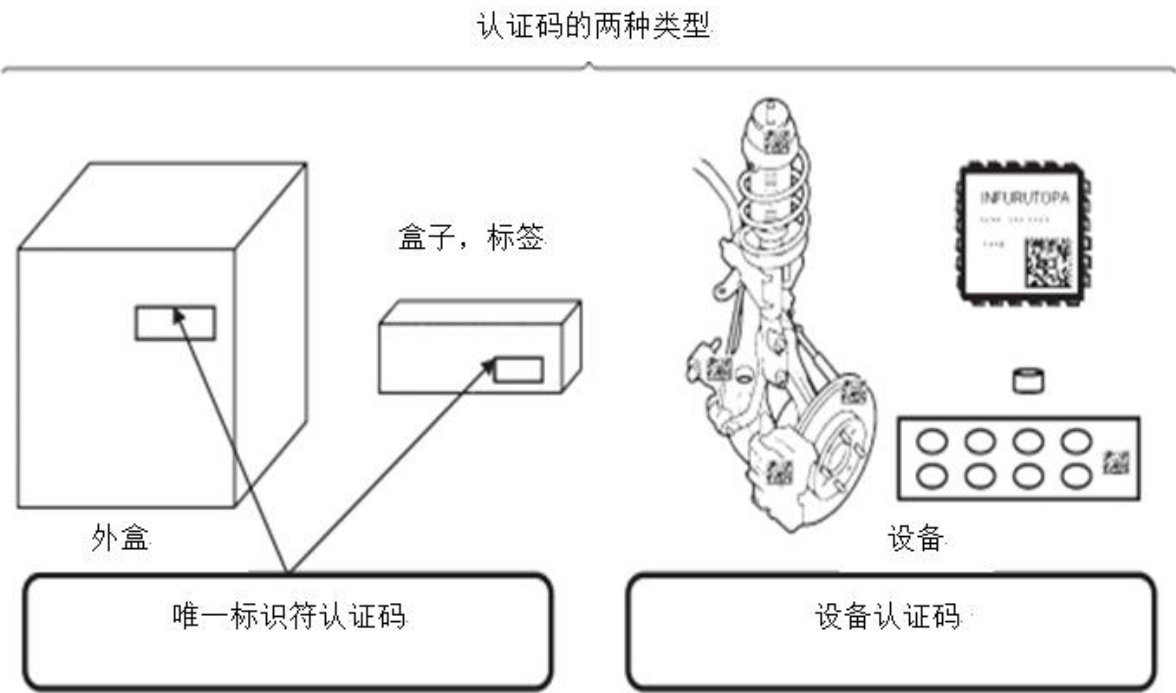


图 A.1 半导体电子签名编码数据集的通用格式

A.2.2 以下示例显示了某个认证机构（相当于电子签名编码数据集方案中的TSP）为设备和唯一标识符签发或注册的认证码的格式和内容：

a) 标识符：参考下述文件：

注：以下文件适用于半导体领域。

——ISO/IEC 15418；

- 自动识别和数据采集技术；
- GS1应用标识符和ASC MH10数据标识符和维护；

——ISO/IEC 15434；

- 自动识别和数据采集技术；
- 大容量ADC媒体的语法；

——ANSI MH10.8.2；

- 数据标识符和应用标识符标准。

b) 唯一编号：根据每个唯一标识符分配的唯一代码。

A.3 使用案例：印花税

A.3.1 图A.2显示了纳税印花ESEDs的示例。



基于可见数字印章（VDS）的纳税印花			
	身份认证要素 1（源 1）	VXB1	
	身份认证要素 1（源 2）	HVBXMJAX	
	...		
	身份认证要素 N（源 N）		
VXB1HVBXMJAX 221 002 06501 PL 1CZ			

图 A.2 基于 AFNOR XP Z42-105 的大规模 DataMatrix 代码中携带电子签名编码数据集的纳税印花示例

A.3.2 用于在独立运行的产品识别和身份认证系统（通常采用不同的编码架构和不同类型的安全特征）之间建立互操作性的一种方法是使用可见数字印章，可见数字印章可以公共或私人二维代码的形式打印在纳税印花上。

A.3.3 ISO 22381:2018建议使用可见数字印章，作为TEP的一部分，以允许所有利益相关者（包括消费者）在无需上网的情况下验证唯一标识符（UID），并访问特定纳税印花上使用的安全特征信息。

A.3.4 以下示例说明了VDS如何与纳税印花和追溯系统结合使用：

- 图 2 显示了一个带有两个不同 DataMatrix 代码的纳税印花示例：较小的代码包含用于单元级跟踪的 UID，较大的代码是可见数字印章；
- 较小的代码在产品生产过程中应用和进行验证，然后由生产商对所有经验证的 UID 列表进行数字签名，生产商必须拥有信用服务提供方颁发的合格数字证书，并将其转移至数据存储库；

- VDS 代码还包含 UID、UID 颁发组织的合格电子签名以及一个安全链接，链接到纳税印花上使用的所有安全特征信息。这使得来自（欧盟）任何成员国的检查员，甚至消费者，都可以检查 UID 和其他数据是否真实且与产品相符；
- 数据结构符合 AFNOR XP Z42-105。

A. 4 使用案例：物联网（IoT）安全和安全符合性证书

A. 4. 1 图A.3显示了物联网VDS的结构。



图 A.3 物联网的可见数字印章

- A. 4. 2 对于每一件物品，物联网制造商必须确保在物联网设备及其外包装上贴上安全和不可移除的唯一身份标识标记，如雕刻的代码或安全标签。
- A. 4. 3 基于此全局系统，使用单个移动应用程序（TEP），来自A国的检查员能够安全地读取由B国、C国或运行特定电子签名编码数据集方案的治理机构所接受的任何其他国家签发的可见数字印章数据。该可见数字印章还包含关于每个生产商/国家使用的认证安全特征的信息和指南（或安全链接）。如此一来，每个国家都可以自由使用不同的技术和方案，因为它们知道VDS互操作功能是为了帮助不熟悉某些国家电子签名编码数据集方案的检查员。
- A. 4. 4 在可信环境中，使用一个通用TEP建立各种跟踪追溯系统的互操作性是一个重要的系统安全要素。这是有效及时发现非法物联网物品的条件之一，避免了非法物联网物品在系统内被接受使用的风险。

A. 5 使用案例：门禁卡

A. 5. 1 图A.4显示了用于数字身份标识的可见数字印章的结构。



图 A.4 数字身份标识的可见数字印章通用格式

A. 5. 2 图A.5显示了可见数字印章数字身份标识基本用例的读取序列。

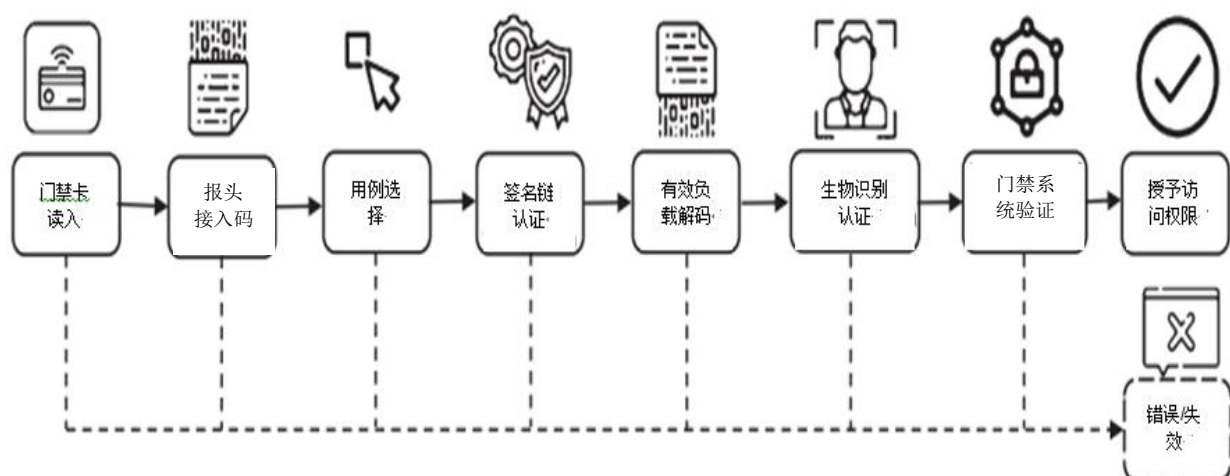


图 A.5 基于可见数字印章的门禁卡（生物识别门禁控制系统）身份验证

A. 5.3 数字身份标识是一个关键领域，文件或访问权限的颁发组织必须是可信的。门禁控制通常涉及使用集中的系统来管理与受保护区域相关的用户、用户权限和角色。访问验证流程基于个人门禁卡，由无人值守系统验证，以及控制操作员对区域访问权限进行物理控制。

A. 5.4 门禁卡必须具有个性化特征，并由正确的机构颁发——在门禁卡访问验证之前须核实颁发机构。

A. 5.5 使用门禁卡中存储的符合AFNOR XP Z42-105标准的数据结构，可以满足门禁卡认证的所有要求。

A. 5.6 当所需的授权数据（个人信息以及UID）获得门禁控制系统的数字签名时（发放门禁卡），身份验证系统（电子或人工）能够验证门禁卡的来源和真实性。在这种情况下，包含生物特征模板（身份证图片、指纹和/或人脸识别模式）的电子签名编码数据集可以作为二进制数据存储在智能门禁卡中和/或以二维条形码的形式打印。当需要获得访问权限时，身份验证系统（TEP）读取门禁卡，根据发卡机构的可信证书验证签名（电子印章），然后对持卡人进行生物特征验证。只有在验证通过之后，才能授予访问权限。

A. 6 使用案例：电子签名编码数据集（VDS）作为一种“了解你的客户（KYC）”的身份验证服务，用于基于区块链或无需连接区块链的分布式账本技术（DLT）的电子文档

A. 6.1 KYC流程包括身份证验证、生物特征验证和文件验证（例如，作为居住证明的水电费账单）。KYC流程必须遵守KYC法规和反洗钱法规，以限制欺诈行为。

A. 6.2 文档的颁发机构将哈希表发布在区块链上。区块链创建一个VDS，其中包含文档的哈希表和文档交付的时间戳。区块链对VDS进行数字签名。

A. 6.3 用户收集颁发机构发送的电子文档和区块链发送的VDS。用户可以验证发送的文档是否是存储在区块链上的文档。

A. 6.4 当客户服务提供商想要验证文档的合法性时，不需要连接到区块链。验证可以在离线模式下使用文档和可见数字印章执行，其中可见数字印章对所需哈希表进行认证。图A.6显示了可见数字印章颁发和区块链参考文档验证的完整流程。

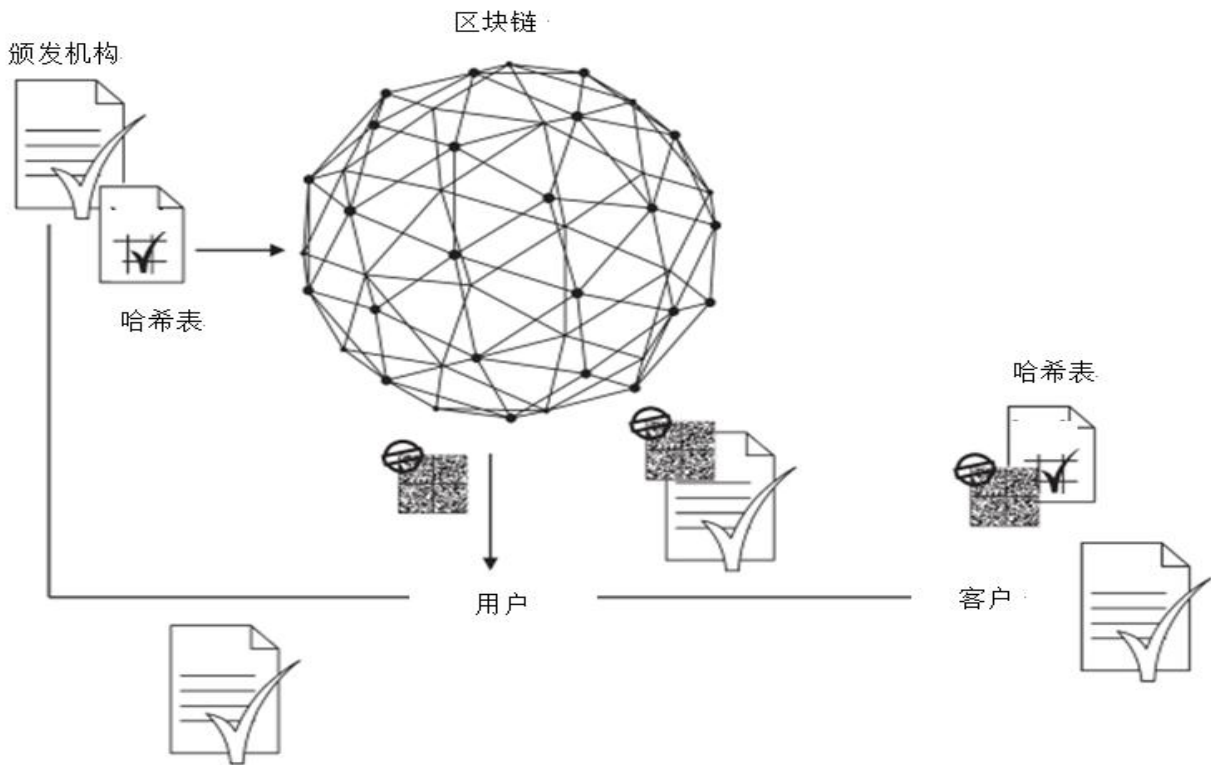


图 A.6 ESEDs 生命周期，包括预先存在的证明

A. 7 使用案例：使用电子签名编码数据集（可见数字印章）通过直接借记进行安全支付

- A. 7.1 此应用由客户的网上银行提出，用于支付通过电子邮件或邮寄收到的发票金额。发票也可用于电子商务网站上的付款。
- A. 7.2 为了签发可见数字印章，债权人在其银行登记，并获得授权开具发票的电子印章证书。债权人开具发票（纸质或电子版；可以是PDF文件），在该发票上通过VDS封装其银行标识符（BIC和IBAN）、发票参考号和发票金额。
- A. 7.3 使用智能手机上的网上银行应用程序，债务人可以：
- 验证债权人身份；
 - 核实发票金额；
 - 通过转账发起付款。
- A. 7.4 发票参考号允许债权人将款额和发票进行明确匹配。付款操作只需单击一次，无需输入债权人的银行详细信息。
- A. 7.5 如果没有可见数字印章，同一设备很可能会受到包含伪造者银行账户信息的伪造邮件的攻击。这种方法在提高工效的同时保证了交易的安全性。使用现有的支付方案（直接借记或即时直接借记），在网银环境下很容易实现。

附录 B

(资料性)

每个目录的可见数字印章方案示例

B.1 概述

本附录举例说明了应由信任服务运营方建立的可见数字印章方案的四个目录。

B.2 目录 1：参与者列表

可见数字印章方案治理机构的参与者列表。

表 B.1 参与者目录

国家	组织注册号	组织名称	状态	联系点

表 B.2 文档历史记录

版本	日期	修改	编辑人员
0.1	2021 年 10 月 15 日	模板创建	编辑人员姓名

B.3 目录 2：可见数字印章方案的 TSPS 列表

可见数字印章方案的信用服务提供方列表。

表 B.3 信用服务提供方目录

国家	组织注册号	组织名称	状态	联系点

表 B.4 文档历史记录

版本	日期	修改	编辑人员
0.1	2021 年 10 月 15 日	模板创建	编辑人员姓名

表B.4 文档历史记录（续）

版本	日期	修改	编辑人员

B.4 目录 3：可见数字印章方案软件创建编辑器列表

可见数字印章方案的软件创建编辑器列表。

表 B.5 可见数字印章软件创建编辑器目录

国家	组织注册号	组织名称	状态	联系点

表 B.6 文档历史记录

版本	日期	修改	编辑人员
0.1	2021 年 10 月 15 日	模板创建	编辑人员姓名

B.5 目录 4：可见数字印章方案软件验证编辑器列表

可见数字印章方案的软件验证编辑器列表。

表 B.7 可见数字印章软件验证编辑器目录

国家	组织注册号	组织名称	状态	联系点

表 B.8 文档历史记录

版本	日期	修改	编辑人员
0.1	2021 年 10 月 15 日	模板创建	编辑人员姓名

表B.8 文档历史记录（续）

版本	日期	修改	编辑人员

参 考 文 献

- [1] ISO 3166-1, 代表国家名称及其附属机构的编号——第1部分: 国家代码
- [2] ISO 22378, 安全性与韧性——产品和文档的真实性、完整性和信任——防止伪造和非法贸易的可互操作物体识别和相关认证系统指南
- [3] ISO 22380, 安全性与韧性——产品和文档的真实性、完整性和信任——产品欺诈风险和对策的一般原则
- [4] ISO 22381:2018, 安全性与韧性——产品和文档的真实性、完整性和信任——建立物体识别系统互操作性以防止伪造和非法贸易的指南
- [5] ISO 22382, 安全性与韧性——产品和文档的真实性、完整性和信任——消费税印花的内容、安全、发行和检查指南
- [6] ISO 22383, 安全性与韧性——产品和文档的真实性、完整性和信任——物资认证解决方案的选择和性能评估指南
- [7] ISO 22384, 安全性与韧性——产品和文档的真实性、完整性和信任——制定和监测保护计划及其实施的指南
- [8] ISO/IEC 9594-8, 信息技术——开放系统互连——第8部分: 目录: 公钥和属性证书框架
- [9] ISO/IEC 15418, 信息技术——自动识别和数据采集技术——GS1应用标识符和ASC MH10数据标识符和维护
- [10] ISO/IEC 15434, 信息技术——自动识别和数据采集技术——大容量ADC媒体的语法
- [11] ISO/IEC 16022, 信息技术——自动识别和数据采集技术——数据矩阵条形码符号规范
- [12] ISO/IEC 20248:2022, 信息技术——自动识别和数据采集技术——数字签名数据结构模式
- [13] AFNOR XP Z42-105:2019, 使用Otentik可见数字印章(VDS)对文件或物体携带的数据进行认证、验证和获取的电子存储规范
- [14] ANSI MH10.8.2, 数据标识符和应用标识符标准
- [15] ETSI TS 102042, 电子签名和基础设施(ESI); 公钥证书颁发机构的政策要求
- [16] ETSI TS 101 903——电子签名和基础设施(ESI); XML高级电子签名(XAdES)
- [17] ETSI TS 102 853——电子签名和基础设施(ESI); 签名验证程序和政策技术规范
- [18] ETSI TS 119 612 V2.1.1——电子签名和基础设施(ESI); 可信列表
- [19] IETF RFC 4387——Internet X.509公钥基础设施操作协议: 通过HTTP访问证书存储
- [20] IETF RFC 4648——Base16、Base32和Base64数据编码
- [21] IETF RFC 5280——Internet X.509公钥基础设施证书和证书吊销列表(CRL)配置文件
- [22] IETF RFC 6960——X.509互联网公钥基础设施在线证书状态协议——OCSP
- [23] ITU-T建议书X.509(2005), 信息技术——开放系统互连——目录: 认证框架, 08/05
- [24] NIST FIPS PUB 180-4——安全哈希表标准(SHS)
- [25] NIST FIPS PUB 186-4——数字签名标准(DSS)
- [26] RFC 3986, 统一资源标识符(URI)
- [27] WebTrust for CA——众多浏览器指定的CA标准