ICS 35.240.60
CCS L 79

中华人民共和国国家标准

GB/T 31308.4—2023/ISO 14533-4:2019

行政、商业和行业中的数据元、过程和文档 长效签名 第4部分:用于长效签名格式的存证对象属性

Processes，data elementsanddocumentsin commerce，industry and administration—Longterm signature—Part4：Attributespointingto proofofexistenceobjectsused in longterm signature formats

(ISO 14533-4:2019，Processes，data elementsanddocumentsin commerce，industry and administration—Longterm signatureprofiles—Part4：Attributes pointingto (external) proofofexistenceobjectsused in longterm signature formats(PoEAttributes)，IDT)

2023-12-28发布 2024-04-01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。

本文件是 GB/T 31308的第 4部分 。GB/T 31308已经发布了以下部分 :

- 商业、工业和行政的过程、数据元和单证　长效签名规范　第 1部分:CMS高级电子签名(CAdES)的长效签名规范(GB/T 31308.1—2014);
- 商业、工业和行政的过程、数据元和单证　长效签名规范　第 2部分:XML高级电子签名(XAdES)的长效签名规范(GB/T 31308.2—2014);
- 行政、商业和行业中的数据元、过程和文档　长效签名　第 3部分:PDF高级电子签名(PAdES)的长效签名规范(GB/T 31308.3—2023);
- 行政、商业和行业中的数据元、过程和文档　长效签名　第 4部分 :用于长效签名格式的存证对象属性(GB/T 31308.4—2023)。

本文件等同采用 ISO 14533-4:2019《行政、商业和行业中的数据元、过程和文档　长效签名规范　第 4部分 :用于长效签名格式的存证对象属性》。

本文件做了下列最小限度的编辑性改动 :

- 将标准名称改为《行政、商业和行业中的数据元、过程和文档 长效签名 第 4部分 :用于长效签名格式的存证对象属性》。

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。

本文件由全国电子业务标准化技术委员会(SAC/TC83)提出并归 口。

本文件起草单位 :杭州电子科技大学、中国标准化研究院、深圳市科标矩阵科技有限公司、浙江永基智能科技有限公司、中科标准(宁德)科技有限公司、福建福昕软件开发股份有限公司、浙江方正印务有限公司、深圳市金政软件技术有限公司、华涛标准技术(杭州)有限公司、皖西学院、深圳市永达电子信息股份有限公司、东莞市惟思德科技发展有限公司、浙江数智交院科技股份有限公司、宁波市标准化研究院。

本文件主要起草人:蒋琤琤、李仕、章建方、张释元、王少康、梁俊义、黄秋华、燕丽、庄跃辉、刘丹、胡金华、石自军、江泳、林影、王益维、章文福、唐娟、吴建港、曾祺惠。

引　言

GB/T 31308是确保实现长效签名的互操作性,使电子签名能够长期验证的标准,对于电子商务市场安全有重大作用。GB/T 31308拟由4个部分构成。

— 第1部分:CMS高级电子签名(CAdES)的长效签名规范。目的在于阐明CMS高级电子签名(CAdES)的长效签名规范,确保该类电子签名能够被长期验证。

— 第2部分:XML高级电子签名(XAdES)的长效签名规范。目的在于阐明XML高级电子签名(XAdES)的长效签名规范,确保该类电子签名能够被长期验证。

— 第3部分:PDF高级电子签名(PAdES)的长效签名规范。目的在于阐明PDF高级电子签名(PAdES)的长效签名规范,确保该类电子签名能够被长期验证。

— 第4部分:用于长效签名格式的存证对象属性。目的在于阐明长效签名验证所需存证对象属性的规范,确保电子签名能够被长期验证。

GB/T 31308(所有部分)均为一一对应采用ISO 14533(所有部分),以保证电子签名长效验证的实施规范与国际接轨。通过制定该系列标准,完善相关标准体系。

行政、商业和行业中的数据元、过程和文档 长效签名 第4部分:用于长效签名格式的存证对象属性

1 范围

本文件规定了用于长效签名格式的存证(PoE, Proofofexistence)属性和对象,描述了PoE基本概念、属性特征,给出了PoE对象的类型、基本字段,以及相关实例。

本文件适用于长效签名格式中所使用的(外部)存证对象,即通过既存可用的数字签名和可信时间值实现长效签名的动态验证。

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。

ISO 32000-2 文件管理 便携式文件格式 第2部分:PDF 2.0(Document management—Portable documentformat—Part2: PDF 2.0)

ISO/IEC 8825-1 信息技术 ASN.1(抽象语法标记,AbstractSyntax Notation)编码规则 基本编码规则(BER)、正则编码规则(CER)、非典型编码规则(DER)规范[Information technology—ASN.1 encoding rules: Specification ofBasic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)]

注:GB/T 16263.1—2006 信息技术 ASN.1编码规则 第1部分:基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)规范(ISO/IEC 8825-1:2002,IDT)

ISO/IEC 9594-8 信息技术 开放系统互连 目录 第8部分:公钥和属性证书框架(Information technology—Open Systems Interconnection—The Directory—Part8:Public-key and attribute certificate frameworks)

注:GB/T 16264.8—2005 信息技术 开放系统互连 目录 第8部分:公钥和属性证书框架(ISO/IEC 9594-8:2001,IDT)

ETSIEN 319 122-1V1.1.1:2016 电子签名和基础设施(ESI) CAdES(CMS高级电子签名,CMS Advanced ElectronicSignatures)数字签名 第1部分:构建模块和CAdES基线签名[ElectronicSigna-

tures and Infrastructures (ESI)；CAdESdigitalsignatures；Part1：Building blocks and CAdESbase- line signatures]

IETF RFC 3161[1)] 时间戳协议(TSP)[Timestamp Protocol (TSP)]

1) 见 https：//tools . ietf. org/html/3161。

IETF RFC 4648[2] Base16、Base32与 Base64数据编码(The Base16，Base32，and Base64 Data Encodings)

IETF RFC 4998[3] 证据记录语法[Evidence Record Syntax(ERS)]

IETF RFC 5652[4] 加密报文语法[Cryptographic Message Syntax(CMS)]

IETF RFC6283[5] 可扩展标记语言证据记录语法[ExtensibleMarkupLanguageEvidenceRecord Syntax(XMLERS)]

IETF RFC 6960[6] 在线证书状态协议 [Online Certificate Status Protocol (OCSP)]

3 术语和定义

ISO/IEC 9594-8、ISO 32000-2、ISO/IEC 8825-1、IETF RFC 3161和 IETF RFC 6960界定的以及下列术语和定义适用于本文件。

ISO 和 IEC为标准化使用所维护的术语数据库,具体网址如下：

—ISO 在线浏览平台：http://www.iso.org/obp;

—IEC 电子术语百科：http://www.electropedia.org/。

3.1

数字签名 digitalsignature

附加在数据字符串上的数据,或是对数据字符串所作的密码变换。用户(如数据字符串的接收方)可以使用这种数据或变换确认数据字符串的来源和完整性,以防止数据字符串被伪造,起到保护数据字符串的目的。

注：本文件中的数字签名还包括根据法规(EU) No910/2014[6] 和 ISO/IEC 9594-8证书、CRL(认证撤销清单,CertificateRevocation List)(见 ISO/IEC9594-8)和配置文件中定义的 OCSP 响应和签名的电子签名、高级电子签名、合格电子签名、电子印章、高级电子印章、合格电子印章、电子时间戳和合格电子时间戳。

[来源 :ISO/IEC 7816-4:2013, 3.21, 有修改]

3.2

文档标识符 documentidentifier;DId

用于机器处理的电子文档的间接标识符,其形式为 IETF RFC 3161所定义的非典型编码规则(DER)编码的 ASN.1类型 MessageImprint(报文印记)。

3.3

文档签名标识符 documentsignature identifier;DSId

用于机器处理的文档签名间接标识符,其形式为 IETF RFC 3161 中所定义的非典型编码规则(DER)编码的 ASN.1类型报文印记(含非对称签名算法的 DER 编码结果)。

示例：已签署电子文档的数字签名(3.1) 中包含的 ECDSA(椭圆曲线数字签名算法,Elliptic Curve Digital Signature Algorithm)或 RSA(Ron Rivest、AdiShamir和 Leonard Adleman三人姓氏的首字母)结果。

注 1：DSId主要用于电子化签署的电子文档的间接机器处理识别，例如，如果 PDF文件包含多个版本的 PDF文档，则 DSId用于 PDF文档识别，这些版本的 PDF文档，是在多个文档时间戳(见 ISO 32000-2:2017，12.8.5)之间采用增量更新(参见 ISO 32000-2:2017，7.5.6)方式创建，或者是在 PDF签名或 PDF文档时间戳之后采用增量更新创建。

注 2：间接标识符是指根据所使用的哈希算法而变化的相对唯一的可变哈希值。当哈希函数的两个不同输入字符串产生相同的哈希结果时，被称为哈希冲突。

---

2) 见 https://tools.ietf.org/html/4648。

3) 见 https://tools.ietf.org/html/4998。

4) 见 https://tools.ietf.org/html/5652。

5) 见 https://tools.ietf.org/html/6283。

6) 见 https://tools.ietf.org/html/6960。

3.4

文档类型标识符 documenttype identifier;DTId

用于标识相关联电子文档格式和内容类型的字符序列。

注：DTId对受数字签名(3.1)保护的电子文档内容的正确解释至关重要。DTId是用于标识文件扩展名或内容类型的值(见 IETF RFC 2231或 IETF RFC 2045)，DTId的值包含在受数字签名保护的字段中(见附录 F)。

3.5

行尾符 end-of-linemarker;EOL marker

标记一行结束的由一至两个字符组成的序列，包括回车符(0Dh)或换行符(0Ah)或其后紧跟换行符的回车符。

3.6

证据记录 evidencerecord;ER

在某段时间内为一个或多个给定数据对象创建的证据集合，可用于证明某数据对象或数据对象组在特定时间内的完整性和存在性。

注：见 IETF RFC 4998，IETF RFC 6283 and ETSISR 019 510。

3.7

长期 longterm

时间段长到技术发生更迭(包括对新媒体和数据格式的支持)以及用户社区出现变化，该技术更迭或变化会对现有知识库中信息产生影响，这种影响可能会延续到无限的未来。

注：密码算法可能变弱。

3.8

长期完整性保存/长期保存 long-term integritypreservation/long-term preservation；LTI

长期保证数字签名(3.1)的有效状态和(或)提供数据长期存在的证据。即使是在加密技术(如加密算法、密钥大小或哈希函数)已过时、密钥泄漏或丧失检查公钥证书有效状态能力的情况下，该有效状态或证据依然有效。

3.9

哈希对象标识符 objectidentifierasa hash；ObjectId

由 DId(3.2)或 DSId(3.3)等对象标识符组成的，PoE对象(3.12)、PoE属性(3.11)或数据对象的哈希引用。

3.10

存证 proofofexistence；PoE

证明一个对象在某特定日期/时间存在的证据。

注：见 ETSISR 019 510。

3.11

存证属性/PoE属性 proofofexistenceattribute/PoE attribute

存证属性是对 PoE对象(3.12)的引用进而明确指明它们的语义,存证属性受 PoE对象保护。该引用包含 PoE对象类型、可选 PoE对象位置、PoE对象的可选存储以及可选的数据对象引用,数据对象引用指的是数据对象附加说明。

注：PoE属性可能是包含 ObjectId(3.9)[例如 DId(3.2)或 DSId(3.3)的数字签名(3.1)或文件的签署或非签署对象]。见 4.1或附录 G,其中 PoE对象的类型是文件扩展名,如包含 PoE对象的“timestampedFile.EXT.TST.DSId”。该文件存储在“timestampedFile.EXT”中。该时间戳存储在时间戳文件“timestampedFile.EXT.TST”中。

3.12

存证对象 proofofexistenceobject

PoE对象 PoE object

表示受保护数据对象的相关信息,如类型、状态或完整性、日期和时间的可靠信息以及数字签名(可能是时间戳的一部分)。它可以证明 PoE对象的完整性和其来源。

注：见 DId(3.2)或 DSId(3.3)。

3.13

可信列表 trusted list；TL

可信实体签名的预定义数据项列表，表内所有数据项经该可信签名实体认证和批准。

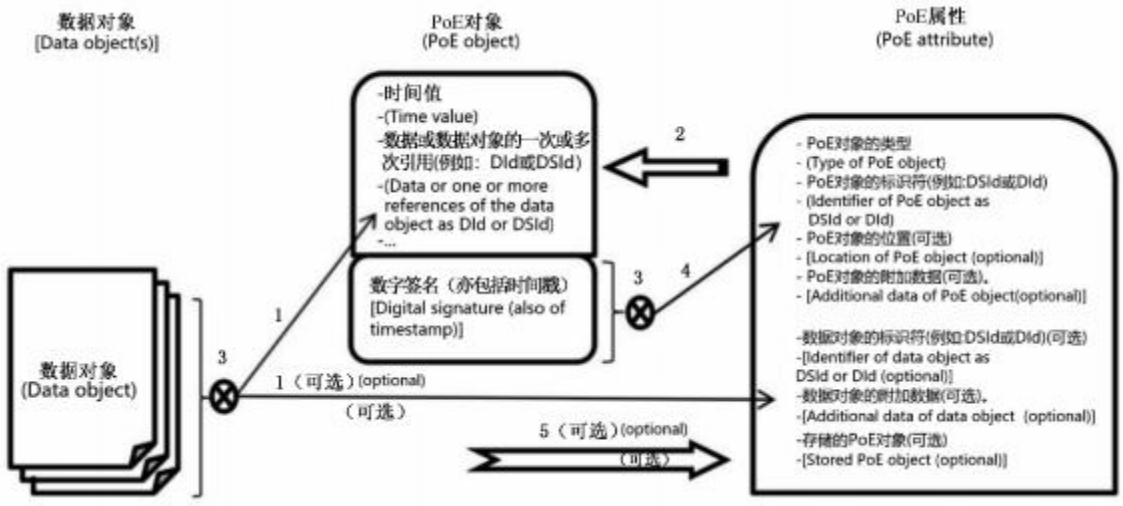
注：TL的主要用途是验证签名对象，使用 TL作为信任锚(可信根证书)的来源，参见 ISO/IEC 9594-8。有关 TL的更多信息，请参阅操作系统文档，例如 Windows、iOS或第 910/2014号欧盟法规[eIDAS(电子身份识别和认证服务，electronic Identification and Authentication Services)法规]。

4 PoE属性

4.1 PoE基本概念

本文档将 PoE属性规定为一个对象，该对象在可选数据对象和可信证据之间提供引用，该可信证据是数据对象或一组数据对象的其中一种属性，该属性可以是在某个特定时间间隔或 日期以及图 1所示时间内数据对象的完整性、状态、数据对象类型或解释类型。PoE属性为包含在签署或非签署属性中的可选对象，作为在 ISO 14533-1、ISO 14533-2、ISO 14533-3中所述的通过使用具有相似字段要素的格式扩展。PoE属性还能以包含 PoE对象的 ObjectId(例如 DId或 DSId)的文件的形式定义，其中 PoE属性的文件名由包含 PoE对象的文件的文件名与附录 G 中所定义的文件扩展名串联而成。

示例：若数据对象文件的文件名为“reports.PNG”，带有时间戳的 PoE对象文件的文件名为“reports.PNG.TST”，则 PoE属性文件的文件名为“reports.PNG.TST.DSId”。



标引序号说明：

1— 存储数据对象哈希值的字段；
2— PoE属性中引用的 PoE对象；
3— 哈希计算；
4— 存储 PoE对象签名哈希值的字段；
5— 能存储在 PoE属性中的 PoE对象。

图 1 PoE概念

PoE对象可在数据对象外部(即为两个独立的对象),称为外部 PoE对象;PoE对象可以包含数据对象;PoE对象也可作为数据对象的一部分。

注 1: PoE对象作为数据对象一部分的一个示例是 PDF文件中包含的 PDF文档时间戳,其中文档时间戳通常通过增量更新的方式进行修改,以保护 PDF文件中所包含的 PDF文档。若该 PDF文档受 PDF文档时间戳或