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 elements and documents in commerce, industry and administration—Long term signature—Part 4: Attributes pointing to proof of existence objects used in long term signature formats

(ISO 14533-4:2019, Processes, data elements and documents in commerce, industry and administration—Long term signature profiles—Part 4: Attributes pointing to (external) proof of existence objects used in long term 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/TC 83)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, Proof of existence)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 document format—Part 2: PDF 2.0)

ISO/IEC 8825-1 信息技术 ASN.1(抽象语法标记,Abstract Syntax 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 of Basic 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—Part 8: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)

ETSI EN 319 122-1 V1.1.1:2016 电子签名和基础设施(ESI) CAdES(CMS高级电子签名,CMS Advanced Electronic Signatures)数字签名 第1部分:构建模块和CAdES基线签名[Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures]

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

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