ICS 35.240.60
CCS L 79

中华人民共和国国家标准

GB/T 31308.3—2023/ISO 14533-3:2017

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

Processes,data elementsanddocumentsin commerce,industry and administration—Longterm signature—Part3:Longterm signature profilesforPDF AdvancedElectronicSignatures(PAdES)

(ISO 14533-3:2017,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 3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 14533-3:2017《商业、行业和行政中的数据元、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》。

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。

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。

本文件起草单位 :杭州电子科技大学、浙江永基智能科技有限公司、中国标准化研究院、中科标准(宁德)科技有限公司、清华大学深圳国际研究生院、福建福昕软件开发股份有限公司、皖西学院、浙江焕华档案管理有限公司、杭州电子科技大学上虞科学与工程研究院有限公司、东莞市中标科技有限公司、杭州市标准化研究院。

本文件主要起草人:蒋琤琤、江泳、李仕、梁俊义、王少康、张释元、章建方、刘丹、李黎、杨余久、叶苏娟、张殿宝、万耀珠、马益洪。

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/T31308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3部分:PDF高级电子签名(PAdES)的长效签名规范

1 范围

本文件规定了PDF高级电子签名(PAdES)的有关要素,以确保数字签名长期可被验证。

本文件不给出数字签名的新技术规范,也不对已有数字签名技术规范的使用提出新的约束。

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 14533-1 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[Processes, data elements and documents in commerce, industry and administration—Long term signatureprofiles—Part1:Long term signatureprofilesforCMSAdvanced ElectronicSignatures (CAdES)]

注: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1部分:CMS高级电子签名(CAdES)的卡效签名规范(ISO 14533-1:2012,IDT)。

ISO 32000-2 文件管理 可移植文件格式 第2部分:PDF 2.0(Document management—Portable documentformat—Part2:PDF 2.0)

3 术语和定义

ISO 14533-1界定的以及下列术语和定义适用于本文件。

3.1

高级电子签名 advanced electronicsignature

与签名人唯一关联的且能够识别签名人的电子签名 。它是用电子签名数据创建的 ,能检测签字后的所有改动 ,签名人能确定他是唯一可以控制该电子签名的人 。

4 符号和缩略语

下列符号和缩略语适用于本文件：

C:条件型

M :必备型

O:可选型

P:禁止型(创建或修改)

CA:认证机构(Certification Authority)

CAdES: CMS高级电子签名(CMS advanced electronic signature)

CMS:加密报文语法(Cryptographic Message Syntax)

CRL:认证撤销清单(Certificate Revocation List)

DSS:文档安全存储(DocumentSecurity Store)

OCSP:联机证书状态协议(Online Certificate Status Protocol)

PAdES:PDF高级电子签名(PDF Advanced Electronic Signatures)

PAdES-A:使用存档验证数据的 PAdES-T(PAdES-T using Archive validation data)

PAdES-DT:只使用文档时间戳字典的 PDF(PDFfileusing onlyDocumentTimestampdictionary)

PAdES-DTA:使用存档验证数据的 PAdES-DT(PAdES-DT using Archive validation data)

PAdES-T:使用时间戳的 PAdES(PAdES using Timestamp)

TSA:时间戳机构(Time-Stamping Authority)

VRI:用于验证的相关信息(Validation Related Information)

5 要求

5.1 PAdES-T数据的生成或验证符合本文件的前提条件是满足以下要求:

a) 应包含本文件所规定的 PAdES-T配置文件中的所有“必备型”要素;

b) 应提供本文件所规定的 PAdES-T配置文件中所有“条件型”要素的详细规范。

5.2 PAdES-A数据的生成或验证符合下列两项要求:

a) 应包含本文件所规定的 PAdES-A配置文件中的所有“必备型”要素;

b) 应提供本文件所规定的 PAdES-A配置文件中所有“条件型”要素的详细规范。

5.3 PAdES-DT和 PAdES-DTA数据的生成或验证应符合附录 B 中图 B.1和图 B.2 中所列要求,见附录 B。

5.4 如果使用了第一方的一致性评定,则实施者应提供符合本文件的一致性声明。声明内容包括披露供应商的一致性声明及其附件(见附录 A),其中附件还应包含实施状态的描述(以及所有“条件型”要素的详细规范)。

注 1:见 ISO/IEC 17050-1:2004。

注 2:图 1给出了 PAdES-T数据和 PAdES-A数据生成和验证的流程设定。

6 长效签名

6.1 PAdES配置文件的定义和流程设定

为了确保电子签名可长期验证,满足以下要求:

— 应可识别签名时间;

— 应能检测到包含签名主体信息和验证数据等各种电子签名信息的任何非法篡改;

— 应确保信息之间的互操作性。

为了满足这些要求,本文件给出了 PAdES的两个配置文件。

a) PAdES-T配置文件:一种用于创建和验证带有时间戳电子签名的配置文件。时间戳存储在该电子签名的“签名时间戳”属性中,或者存储在随后过程中包含了该时间戳的任意对象中,该对

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：
https://d.book118.com/935344340203011301