ICS 35.240.60
L 79

中华人民共和国国家标准

GB/T 31308.2—2014/ISO 14533-2:2012

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

Processes, data elements and documents in commerce, industry and administration—Long term signature profiles—Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)

(ISO 14533-2:2012, IDT)

2014-12-05 发布　　2015-04-15 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 31308《商业、工业和行政的过程、数据元和单证　长效签名规范》由两部分组成：

——第1部分：CMS高级电子签名(CAdES)的长效签名规范；

——第2部分：XML高级电子签名(XAdES)的长效签名规范。

本部分为GB/T 31308的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分等同采用ISO 14533-2:2012《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》。本部分对国际标准的第1章“范围”进行了如下编辑性修改：范围的部分内容改为“注1”。

本部分由全国电子业务标准化技术委员会(SAC/TC 83)归口。

本部分起草单位：厦门英诺尔电子科技股份有限公司、中国标准化研究院、上海新景程物流国际物流有限公司、中国国际电子商务有限公司、四川锦程国际货运代理有限责任公司、深圳市坤鑫国际货运代理有限公司、广东华光国际货运代理有限公司。

本部分主要起草人：张荫芬、李金华、李小林、胡涵景、陈峥、胡荣、曾真、李红兵、姚树红。

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

1 范围

本部分规定了在XML高级电子签名(XAdES)中定义的用于长期进行数字签名验证的数据元。

本部分适用于商业、工业和行政的过程、数据元和单证的XAdES长效签名。

注1:本部分既没有给出数字签名本身的技术规范,也没有对现有的数字签名规范的使用进行限制。

注2:XML高级电子签名(XAdES)是目前广泛使用的XML电子签名语法的扩展。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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 用于商业、工业和行政中的过程、数据元和单证 长效签名规范 第1部分:高级CMS电子签名(CAdES)用长效签名规范

ETSI TS 101 903 v1.4.1(2009-06) XML高级电子签名(XAdES)(XML Advanced Electronic Signatures)[1)]

3 术语和定义

下列术语和定义适用于本文件。

3.1

XML签名 XML signature

所指定报文的签名语法和处理过程。

注:在2002年2月12日发布的万维网(W3C)建议书中定义。

3.2

XML高级电子签名 XML advanced electronic signature;XAdES

在ETSI TS 101 903中定义的能够识别签名人并能检测出非法数据篡改的用于高级XML电子签名的通用术语。

3.3

带有时间的XAdES XAdES with time;XAdES-T

在ETSI TS 101 903中定义的带有确定的签名时间信息的XML高级电子签名。

示例:签名时戳。

---

1) 该标准可从以下网址获得<http://pdaetsi.org/pda/queryform.asp>。