ICS 35.240.60
L 79

中华人民共和国国家标准

GB/T 31308.1—2014/ISO 14533-1:2012

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

Processes, data elements and documents in commerce, industry and administration—Long term signature profiles—Part 1: Long term signature profiles for CMS Advanced Electronic Signatures(CAdES)

(ISO 14533-1:2012, 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1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 14533-1:2012《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》。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1部分:CMS高级电子签名(CAdES)的长效签名规范

1 范围

本部分规定了在CMS高级电子签名(CAdES)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CAdES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:CMS高级电子签名(CAdES)是目前广泛使用的加密报文语法(CMS)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。

ETSI TS 101 733 v1.8.1(2009-11) 电子签名与基础设施(ESI) CMS高级电子签名(CAdES)[Electric Signatures and Infrastructures(ESI);CMS 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

长效签名 long term signature

用于长期进行验证的签名,通过对签名时间、签名主体、以及签名的有效数据等的检测,验证签名信息是否被非法篡改。

3.2

规范 profile

为保证与所引用规范中可选数据元以及可选数据元的取值范围等相关的互操作性所使用的规则。

3.3

要求级别 required level

实现构成规范的数据元所需的级别。

3.4

加密报文语法 cryptographic message syntax;CMS

与所给出报文的签名、摘要、鉴别以及加密相关的语法。

注:在IETF RFC 3852中定义了CMS。

3.5

CMS高级电子签名 CMS advanced electronic signature;CAdES

在ETSI TS 101 733中定义的用于识别签名者和检测非法数据篡改的电子签名。

---

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