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>。

3.6

带有时间的 CAdES　CAdES with time;CAdES-T

在 ETSI TS 101 733 中定义的带有确定签名时间信息的 CMS 高级电子签名。

示例:签名时戳。

3.7

归档的 CAdES　archival CAdES;CAdES-A

在 ETSI TS 101 733 中定义的带有签名主体和有效数据等,用于检测与签名相关的任何非法数据篡改信息的 CMS 高级电子签名。

示例:存档时戳。

3.8

内容信息　content information

规定 CMS 中内容的数据结构。

3.9

签名数据　signed data

规定 CMS 中签名数据或相关数据的数据结构。

3.10

签名者信息　signerInfo

规定每个签名者签名信息或相关数据的数据结构。

3.11

签名属性　signed attribute

构成签名主体的签名信息。

3.12

非签名属性　unsigned attribute

不含在签名主体中的签名信息。

注:签名时戳、存档时戳是非签名属性。

3.13

有效数据　validation data

用于验证签名及时戳的证书和证书撤销的信息。

3.14

时戳机构　time stamping authority;TSA

授权的可信第三方机构,提供某个时间点之前数据是否存在的证明。

3.15

时戳标记　time stamp token;TST

将某一数据表示与某一特定时间绑定在一起的数据客体,由此建立该数据在该时间之前已经存在的证据。

3.16

签名时戳　signature timestamp

为识别签名的时间,附加在签名值上的时戳。

3.17

归档时戳　archive timestamp

附加在签名主体和签名的有效数据等有关签名信息上的时戳,以便能够检测出签名信息是否被非法篡改。

3.18

信任锚 trust anchor

验证方用于验证电子签名的以公钥证书或公钥形式提供的信赖源，通常公钥证书由所信赖的源认证机构签发。

3.19

可信第三方机构 trusted third party;TTP

与安全活动相关的另一实体委托的安全机构或其代理。

3.20

认证机构 certification authority;CA

受委托进行开发和分配公钥证书的机构。

注：认证机构可以向实体分配密钥。

3.21

证书 certificate

由认证机构为防止伪造而签发的作为实体的非对称密钥对的一部分的公钥信息。

3.22

属性证书 attribute certificate

包含了职业、资格、职位和其他属性及属性值的证书。

3.23

撤销信息 revocation information

认证机构在有效期内撤销所签发的证书的信息。

注：该信息用于确定证书是否仍然有效。

3.24

增强安全服务 enhanced security service;ESS

与签名相关的可选的增强服务，包括但不仅限于识别签发证书的信息和说明签名类型的信息。

4 符号

下面表示“要求级别”的符号适用于本文件。

——C 条件型；

——M 必备型；

——O 可选型。

5 要求

5.1 CAdES-T 数据的生成或验证应符合本部分给出的下列两项要求：

a) 应包含本部分规定的 CAdES-T 规范中所有要求级别为“必备型”的数据元；

b) 应给出本部分规定的 CAdES-T 规范中所有要求级别为“条件型”的与数据元相关的详细规范。

5.2 CAdES-A 数据的生成或验证应符合本部分给出的下列两项要求：

a) 应包含本部分规定的 CAdES-A 规范中所有要求级别为“必备型”的数据元；

b) 应给出本部分规定的 CAdES-A 规范中所有要求级别为“条件型”的与数据元相关的详细规范。

5.3 当使用甲方一致性评定时，实施方应通过披露供应商的合规声明及附件（见附录 A），做出一个符

合本部分的声明，该合规声明包括实施状态描述(以及条件型数据元的规范)。

注：图1给出了CAdES-T和CAdES-A生成和验证的位置。

6 长效签名规范

6.1 已定义的规范

为使电子签名进行长期验证，签名时间应可识别，包括签名主体信息和验证数据在内的非法篡改信息应可检测，同时保证互操作性。为了满足这些要求，本部分定义了CAdES的两个规范：

a) CAdES-T规范：与CAdES-T数据生成和验证相关的规范；

b) CAdES-A规范：与CAdES-A数据生成和验证相关的规范。

图1给出了CAdES-T数据和CAdES-A数据之间的关系。

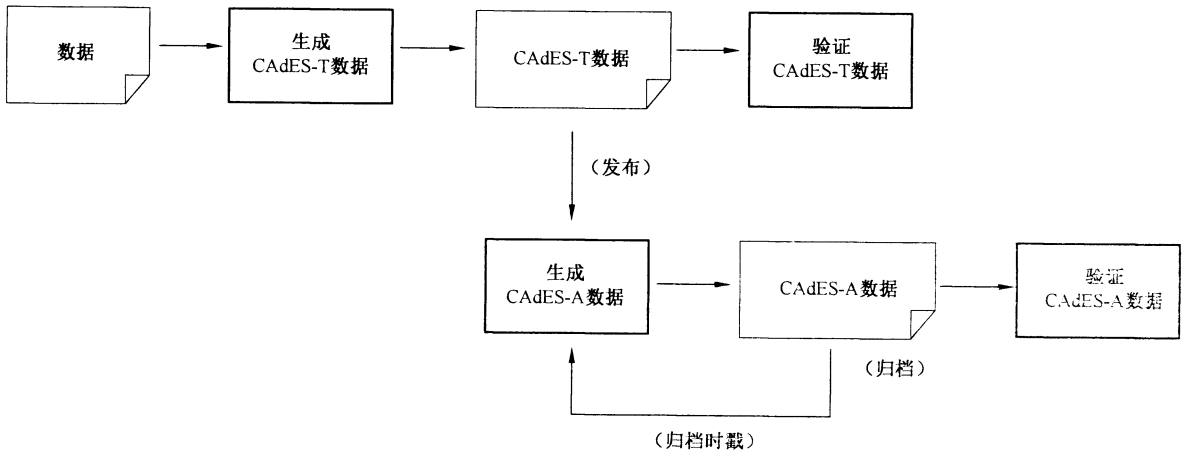

图1 CAdES-T数据和CAdES-A数据之间的关系

6.2 要求级别的表示法

本部分针对构成CAdES-T数据和CAdES-A数据(按照某一规范)，定义了每一项数据元的要求级别的表示法：

a) 必备型(M) 要求级别为“必备型”的数据元是应使用的数据元。如果“必备型”数据元有可选的子数据元，则应至少有一个子数据元是可选的。当选择一个可选数据元时，任何要求级别为“必备型”并且它又是一个可选子数据元的数据元应是可选的。

b) 可选型(O) 要求级别为“可选型”的数据元是由实施方自行决定是否使用的数据元。

c) 条件型(C) 要求级别为“条件型”的数据元是由实施方自行决定是否使用并分别给出如何处理它们的详细规范的数据元。

6.3 要求级别的设置标准

构成CAdES-T和CAdES-A数据的数据元要求级别应符合以下要求：

a) CAdES中定义的要求级别为“必备型”的数据元，以及长效签名的生成和验证必要的数据元，要求级别应是“必备型”。在CAdES中定义的要求级别为“可选型”的数据元可以定义为“必备型”、“可选型”或“条件型”。

b) 外部定义的数据元要求级别应是“条件型”。

示例：OtherCertificateFormat(其他证书格式)。

c) 与确定的应用互动的数据元，要求级别应是“条件型”。

示例：ContentReference（内容参考）。

d) 带有关联条件的数据元，要求级别应是“条件型”。

示例：AttributeCertificate（属性证书），TimeMark（时间标志）。

注：ISO/IEC 18014-2 中定义的归档类型时戳包括在“Time mark or other method(时间标志或其他方法)”中。

e) 仅包含参考信息的数据元，要求级别应是“可选型”。

6.4 未配置的可选数据元的处置

当验证处理所使用的 CAdES 数据包含未配置的数据元时，应采取下列措施：

a) 当上一级数据元的要求级别为“必备型”，并且一个或多个从属的可选数据元将被选定时，或者一个或多个相关的可选数据元将被选定时，应提醒验证方对上述数据元的验证需求进行配置，否则验证无法完成。

示例：在验证处理时，仅在处理位于“RevocationValues(撤消值)”中所使用的“CertificateList(证书列表)”数据元的位置检测“BasicOCSPResponse(基本 OCSPR 响应)”数据元。

b) 当“CounterSignature(附属签名)”是一个未配置的数据元时，应提醒验证方对上述数据元的验证需求进行配置，否则验证无法完成。

c) 并非上述规定的可选数据元可忽略。

6.5 CAdES-T 规范

6.5.1 概述

在 6.5.2、6.5.3 和 6.5.4 中规定了构成 CAdES-T 数据元的要求级别。

6.5.2 内容信息

表 1 规定了构成内容信息数据元的要求级别。

表 1 内容信息

数据元	要求级别	值	ETSI TS 101 733 v1.8.1 参考
ContentType(内容类型)	M	人名—签名数据	5.3
Content(内容)	M	签名数据	5.3

6.5.3 签名数据和签名人信息

表 2 和表 3 规定了构成签名数据和签名人信息数据元的要求级别。

表 2 签名数据

数据元	要求级别	ETSI TS 101 733 v1.8.1 参考
CMSVersion(CMS 版本号)	M	5.4
DigestAlgorithmIdentifiers(摘要算法标识符)	M	5.4
EncapsulatedContentInfo(封装内容信息)	M	5.4
eContentType(电子内容类型)	M	5.4
eContent(电子内容)	O	5.4

表 2（续）

数据元	要求级别	ETSI TS 101 733 v1.8.1 参考
CertificateSet(证书集合)	O	5.4
Certificate(证书)	O	5.4
AttributeCertificateV2(属性证书版本 2)	C	5.4
OtherCertificateFormat(其他证书格式)	C	5.4
RevocationInfoChoices(撤消信息选择)	O	5.4
CertificateList(证书列表)	O	5.4
OtherRevocationInfoFormat(其他撤消信息格式)	C	5.4
SignerInfos(签名人信息)	M	5.4
Single(单个)	O	5.4
Parallel(多个)	O	5.4

表 3　签名人信息

数据元	要求级别	参考 ETSI TS 101 733 v1.8.1
CMSVersion(CMS 版本号)	M	5.6
SignerIdentifier(签名人标识符)	M	5.6
IssuerAndSerialNumber(签发人和序列号)	O	5.6
SubjectKeyIdentifier(主体密钥标识符)	O	5.6
DigestAlgorithmIdentifier(摘要算法标识符)	M	5.6
SignedAttributes(签名属性)	M	5.6
SignatureAlgorithmIdentifier(签名算法标识符)	M	5.6
SignatureValue(签名值)	M	5.6
UnsignedAttributes(非签名属性)	M	5.6

6.5.4　签名属性和非签名属性

表 4 和表 5 规定了构成签名属性和非签名属性数据元的要求级别。要求级别为“条件型”的签名属性和非签名属性数据元不列入表 4 和表 5。

注：非签名属性并不包含在表 4 和表 5，也不限于在表 6 所列的如“Com(完整证书参考)”和“Com(完整撤消参考)”。增加到 CAdES-T 数据中的“完整证书参考”和“完整撤消参考”可以按照 CAdES-T 规范，通过针对这些数据元单独处理与 CAdES-T 规范保持一致。

表 4　签名属性

数据元	要求级别	ETSI TS 101 733 v1.8.1 参考
ContentType(内容种类)	M	5.7.1
MessageDigest(报文摘要)	M	5.7.2

表 4（续）

数据元	要求级别	ETSI TS 101 733 v1.8.1 参考
SigningCertificateReference(签名证书参考)	M	5.7.3
ESS SigningCertificate(ESS 签名证书)	O	5.7.3.1
ESS SigningCertificate v2(ESS 签名证书参考版 2)	O	5.7.3.2
OtherSigningCertificate(其他签名证书)	C	5.7.3.3
SignaturePolicyIdentifier(签名策略标识符)	C	5.8.1
SigningTime(签名时间)	O	5.9.1
ContentReference(内容参考)	C	5.10.1
ContentIdentifier(内容标识符)	C	5.10.2
ContentHints(内容提示)	C	5.10.3
CommitmentTypeIndication(承诺类型指示)	C	5.11.1
SignerLocation(签名人地点)	C	5.11.2
SignerAttribute(签名人属性)	C	5.11.3
ContentTimestamp(内容时戳)	C	5.11.4

表 5　非签名属性

数据元	要求级别	参考 ETSI TS 101 733 v1.8.1
CounterSignature(附属签名)	O	5.9.2
Trusted time(可信时间)	M	4.4.1
SignatureTimeStamp(签名时戳)	O	6.1.1
Time Mark or other method(时间标志或其他方式)	O	4.4.1

6.6　CAdES-A 规范

6.6.1　概述

在 6.6.2、6.6.3 中规定了构成 CAdES-T 数据的数据元要求级别。

6.6.2　CAdES-A 规范的结构

CAdES-A 规范被定义为扩展形式的 CAdES-T 规范加上表 6 中规定的非签名属性。与 CAdES-T 对应部分的各数据元要求级别应在 6.5 中规定。

6.6.3　附加的非签名属性

附加非签名属性的数据元要求级别应在表 6 中说明。对于没有在表 6 规定的数据元要求级别应为“条件型”。

表 6 附加的非签名属性

数据元	要求级别	ETSI TS 101 733 v1.8.1 参考
CompleteCertificateReferences(完整证书参考)	M	6.2.1
CompleteRevocationReferences(完整撤消参考)	M	6.2.2
CompleteRevRefs CRL(完整撤消参考 CRL)	O	6.2.2
CompleteRevRefs OCSP(完整撤消参考 OCSP)	O	6.2.2
OtherRevRefs(其他完整撤消参考)	C	6.2.2
Attribute certificate references(属性证书参考)	C	6.2.3
Attribute revocation references(属性撤消参考)	C	6.2.4
CertificateValues(证书值)	M	6.3.3
CertificateValues(证书值)	O	6.3.3
Certificates maintained by trusted service(由可信服务机构维护的证书)	C	[a]
RevocationValues(撤消值)	M	6.3.4
CertificateList(证书列表)	O	6.3.4
BasicOCSPResponse(基本 OCSP 响应)	O	6.3.4
OtherRevVals(其他撤消值)	C	6.3.4
Certificates maintained by trusted service(由可信服务机构维护的证书)	C	[a]
CAdES-C-timestamp(CAdES-C 时戳)	C	6.3.5
Timestamped cert and crls reference(带时戳的证书和撤消信息选择)	C	6.3.6
Archiving(归档)	M	6.4
ArchiveTimestamp id-aa-48(归档时戳 id-aa-48)	O	6.4.1
ArchiveTimestamp id-aa-27(归档时戳 id-aa-27)	O	[b]
Evidence Record(证据记录)	O	[c]
Other method(其他方式)	C	[d]

[a] 如果委托认证机构(CA)或其他可信机构进行归档期间的证书维护,则无需持有带签名的证书。相反该数据元由于互操性的原因以及防止签名中包含多个相同大小的 CRL 或 OCSP,可以使用在 CMS(表 2)中定义的数据元证书集合或撤消信息选择。

[b] 在 ETSI TSA 101 733 v1.4.0 或更早版本中定义。

[c] 在 IETF RFC 4998 中的定义。

[d] 如果委托其他可信的服务机构进行归档期间维护,则使用该数据元。

6.7 时戳验证数据

对之前时戳的验证需要依靠信任锚的认证和撤证信息。时戳验证数据需要证书链中的各项证书,从 TSA 证书到信任锚证书以及属于每一项这类证书的撤销信息。

如下所述,验证数据可以随 CAdES-A 数据一起存放。不与 CAdES-A 数据一起存放时,验证数据

应当通过另一安全方法存放，包括但不限于由 CA 作为 TTP 或由 TSA 储存。

在对之前的时戳进行验证中，验证数据按照下述方法存放，或另行使用其他安全方法进行存放。

附录 B 规定了与时戳标记结构相关的要求。

a) 签名时戳的验证数据应当在下列生成时的某一处所或由 CA 等机构予以保存。

1) 非签名属性中的数据元如下：

——CertificateValues(证书值)

——RevocationValues(撤销值)

2) 在签名时戳中时间标记(签名时戳标记)数据元如下：

——CertificateSet(证书集合)

——RevocationInfoChoices(撤消信息选择)

3) 签名时戳标记中非签名属性数据元如下：

——CertificateValues(证书值)

——RevocationValues(撤销值)

注：上述 1)和 2)中的数据元在 CMS 中进行定义，3)中的数据元则在 CAdES 中定义。

b) 归档时戳验证数据应在下列生成时的某一处所或由 CA 等机构予以保存。

1) 在归档时戳中时间标记(归档时戳标记)数据元如下：

——CertificateSet(证书集合)

——RevocationInfoChoices(撤消信息选择)

2) 归档时戳标记中非签名属性数据元如下：

——CertificateValues(证书值)

——RevocationValues(撤销值)

注：上面 1)中的数据元在 CMS 中进行定义，2)中的数据元在 CAdES 中定义。

附 录 A
（规范性附录）
提供方一致性声明及其附件

A.1 概述

本附录给出了提供方与CAdES长效签名规范一致性声明的格式。

A.2 提供方一致性声明格式

提供方与长效签名规范一致性声明
编号_____
签发人姓名_____
签发人地址_____

声明的对象：
上面所描述的声明的对象与下面长效签名规范的要求一致。
CAdES-T规范和/或CAdES-A规范。
A.3规定了所使用的数据元。
附加信息：
（操作检查的结果等可以写在此处）
签名人和代表在此签名：

_____
_____
（签发地点和日期）

_____
（姓名，头衔）

A.3 提供方一致性声明的附件格式

A.3.1 概述

提供方一致性声明的附件应包括从A.3.2到A.3.7的条款。

A.3.2 所引用的ETSI TS 101 733版本号

A.3.3 规范实施的范围

表 A.1 规范实施

规范标识符	生成方	验证方
CAdES-T		
CAdES-A		

A.3.4 与 CAdES-T 规范的一致性

表 A.2 签名数据

数据元	要求级别	生成方	验证方
CMSVersion(CMS 版本)	M		
DigestAlgorithmIdentifiers(摘要算法标识符)	M		
EncapsulatedContentInfo(封装内容信息)	M		
eContentType(电子内容类型)	M		
eContent(电子内容)	O		
CertificateSet(证书集合)	O		
Certificate(证书)	O		
AttributeCertificateV2(属性证书 V2)	C		
OtherCertificateFormat(其他证书格式)	C		
RevocationInfoChoices(撤消信息选择)	O		
CertificateList(证书列表)	O		
OtherRevocationInfoFormat(其他撤消信息格式)	C		
SignerInfos(签名人信息)	M		
single(单个)	O		
parallel(多个)	O		

表 A.3 签名人信息

数据元	要求级别	生成方	验证方
CMSVersion(CMS 版本)	M		
SignerIdentifier(签名人标识符)	M		
IssuerAndSerialNumber(签发人和序列号)	O		
SubjectKeyIdentifier(主体密钥标识符)	O		
DigestAlgorithmIdentifier(摘要算法标识符)	M		
SignedAttributes(签名属性)	M		
SignatureAlgorithmIdentifier(签名算法标识符)	M		
SignatureValue(签名值)	M		
UnsignedAttributes(非签名属性)	M		

表 A.4 签名特性

数据元	要求级别	生成方	验证方
ContentType(内容类型)	M		
MessageDigest(报文摘要)	M		
SigningCertificateReference(签名证书参考)	M		
ESSSigningCertificate(ESS 签名证书)	O		
ESS SigningCertificate v2(ESS 签名证书 v2)	O		
OtherSigningCertificate(其他签名证书)	C		
SignaturePolicyIdentifier(签名策略标识符)	C		
SigningTime(签名时间)	O		
ContentReference(内容参考)	C		
ContentIdentifier(内容标识符)	C		
ContentHints(内容提示)	C		
CommitmentTypeIndication(承诺类型指示)	C		
SignerLocation(签名人地点)	C		
SignerAttribute(签名人属性)	C		
ContentTimestamp(内容时戳)	C		

表 A.5 非签名特性

数据元	要求级别	生成方	验证方
CounterSignature(附属签名)	O		
Trusted signing time(可信赖的签名时间)	M		
SignatureTimeStamp(签名时戳)	O		
Time Mark or other method(时间标记或其他方式)	O		

A.3.5 与 CAdES-A 规范的一致性

表 A.6 附加非签名特性

数据元	要求级别	生成方	验证方
CompleteCertificateReferences(完整的证书参考)	M		
CompleteRevocationReferences(完整撤消参考)	M		
CompleteRevRefs CRL(完整撤消参考 CRL)	O		
CompleteRevRefs OCSP(完整撤消参考证 OCSP)	O		
OtherRevRefs(其他撤消参考)	C		
Attribute certificate references(属性证书参考)	C		

表 A.6(续)

数据元	要求级别	生成方	验证方
Attribute revocation references(属性撤消参考)	C		
CertificateValues(证书值)	M		
CertificateValues(证书值)	O		
Certificates maintained by trusted service(由可信服务机构维护的证书)	C		
RevocationValues(撤消值)	M		
CertificateList(证书列表)	O		
BasicOCSPResponse(基本 OCSP 响应)	O		
OtherRevVals(其他撤消值)	C		
Certificates maintained by trusted service(由可信服务机构维护的证书)	C		
CAdES-C-timestamp(CAdES-C-时戳)	C		
Timestamped cert and crls reference(带时戳的证书和撤消信息选择)	C		
Archiving(归档)	M		
ArchiveTimestamp id-aa-48(归档时戳 id-aa-48)	O		
ArchiveTimestamp id-aa-27(归档时戳 id-aa-27)	O		
Evidence Record(证据记录)	O		
Other method(其他方式)	C		

A.3.6 “条件型”数据元所引用的规范

编号	数据元名称	所引用的规范
1.		
2.		

注：表 A.2 至表 A.6 给出了作为“条件型”标识出的数据元名称和所引用的规范。

A.3.7 备注

附 录 B
（规范性附录）
时戳标记的结构

B.1 概述

本附录给出了长效签名时戳结构要求。

B.2 规范性说明

本部分中的签名时戳标记和归档时戳标记应符合 CMS，TSP，CAdES。

注：在 IETF RFC 3161 中定义了 TSP。

B.3 构成数据元的要求级别

在表 B.1 中规定了签名时戳标记各数据元和归档时戳标记各数据元的要求级别。

表 B.1 时戳标记各数据元的要求级别

数据元	要求级别	值
ContentType(内容类型)	M	id-signedData
Content(内容)	M	Signed Data
CMSVersion(CMS 版本)	M	
DigestAlgorithmIdentifiers(摘要算法标识符)	M	
EncapsulatedContentInfo(封装内容信息)	M	
eContentType(电子内容类型)	M	id-ct-TSTInfo
eContent(电子内容)	M	DER-encoded value of TSTInfo
CertificateSet(证书集合)	O	
Certificate(证书)	O	
AttributeCertificateV1(属性证书 V1)	O	
AttributeCertificateV2(属性证书 V2)	O	
OtherCertificateFormat(其他证书格式)	O	
RevocationInfoChoices(撤消信息选择)	O	
CertificateLis(证书列表)	O	
OtherRevocationInfoFormat(其他撤消信息格式)	O	
SignerInfos(签名人信息)	M	
SignerInfo(签名人信息)	M	
CMSVersion(CMS 版本)	M	

表 B.1（续）

数据元	要求级别	值
SignerIdentifier(签名人标识符)	M	
IssuerAndSerialNumber(签发人和序列号)	O	
SubjectKeyIdentifier(主体密钥标识符)	O	
DigestAlgorithmIdentifier(摘要算法标识符)	M	
SignedAttributes(签名属性)	M	
ContentType(内容类型)	M	id-ct-TSTInfo
MessageDigest(报文摘要)	M	
SigningCertificateReference(签名证书参考)	M	
ESS SigningCertificate(ESS 签名证书)	O	
ESS SigningCertificate v2(ESS 签名证书 v2)	O	
OtherSigningCertificate(其他签名证书)	C	
SignatureAlgorithmIdentifier(签名算法标识符)	M	
SignatureValue(签名值)	M	
UnsignedAttributes(非签名属性)	O	
CompleteCertificateReferences(完整证书参考)	O	
CompleteRevocationReferences(完整撤消参考)	O	
CompleteRevRefs CRL(完整撤消参考 CRL)	O	
CompleteRevRefs OCSP(完整撤消参考 OCSP)	O	
CertificateValues(证书值)	O	
CertificateValues(证书值)	O	
Storage of the certificate by CA(认证机构保存的证书)	C	
RevocationValues(撤消值)	O	
CertificateList(证书列表)	O	
BasicOCSPResponse(基本 OCSP 响应)	O	
OtherRevVals(其他撤消值)	C	

参 考 文 献

[1] ISO/IEC 9594-8, Information technology—Open Systems Interconnection—The Directory—Part 8: Public-key and attribute certificate frameworks

[2] ISO/IEC 18014-2, Information technology—Security techniques—Time-stamping services—Part 2: Mechanisms producing independent tokens

[3] IETF RFC 5652, Cryptographic Message Syntax (CMS), Available from <http://www.ietf.org/>

[4] IETF RFC 3161, Time-Stamp Protocol (TSP), Available from <http://www.ietf.org/>

[5] IETF RFC 5940, Additional Cryptographic Message Syntax (CMS) Revocation Information Choices, Available from <http://www.ietf.org/>

[6] IETF RFC 4998, Evidence Record Syntax (ERS), Available from <http://www.ietf.org/>

中 华 人 民 共 和 国
国 家 标 准
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/ISO 14533-1:2012
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室：(010)64275323 发行中心：(010)51780235
读者服务部：(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.5 字数 31 千字
2014 年 12 月第一版 2014 年 12 月第一次印刷
*
书号：155066·1-50420 定价 24.00 元

GB/T 31308.1-2014

打印日期：2015年1月20日 F009A