

ICS 35.240.60
CCS L 79



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 31308.1-2026

Replacing GB/T 31308.1-2014

**Processes, data elements and documents in commerce,
industry and administration - Long term signature - Part 1:
Profiles for CMS Advanced Electronic Signatures (CAAdES)**

行政、商业和行业中的数据元、过程和文档 长效签名 第1部分：CMS高级电子签名（CAAdES）规范

(English Translation)

Issued on: January 28, 2026

Implemented on: May 1, 2026

Issued by: State Administration for Market Regulation

Table of Contents

Preface
Introduction
1 Scope
2 Normative References
3 Terms and Definitions
4 Symbols
5 Requirements
6 Long-term signature standards
6.1 Defined Configuration Files
6.2 Notation of Requirement Levels
6.3 Standards for Setting Requirement Levels
6.4 Handling of Unconfigured Optional Data Elements
6.5 CAdES-T Configuration File
6.6 CAdES-A Configuration File
6.7 Timestamp Verification Data
Appendix A (Informative) Provider's Declaration of Conformity and its Annex
A.1 Overview
A.2 Provider's Declaration of Conformity Format

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part 1: Structure and Drafting Rules of Standardization Documents".

Drafting.

This document is Part 1 of GB/T 31308 "Long-term signatures for data elements, processes and documents in administration, commerce and industry".

GB/T 31308 has published the following parts.

---Part 1: CMS Advanced Digital Signature (CAdES) Specification;

---Part 2: XML Advanced Electronic Signature (XAdES) Specification;

---Part 3: Long-lasting signature specifications for PDF Advanced Digital Signatures (PAdES);

---Part 4: Attributes of evidence storage objects used for long-term signature formats.

This document replaces GB/T 31308.1-2014 "Specification for Long-Term Signatures of Processes, Data Elements and Documents in Commercial, Industrial and Administrative Sectors" (Chapter 1).

Part 1: Long-Term Signature Specification for CMS Advanced Electronic Signatures (CAAdES), compared with GB/T 31308.1-2014, except for structural adjustments and compilation...

Aside from the logical changes, the main technical changes are as follows.

- a) The scope has been changed (see Chapter 1, Chapter 1 of the 2014 edition);
- b) The term "specification" has been changed to "configuration file" (see 3.2, 2014 version 3.2);
- c) The term "valid data" has been changed to "validation data" (see 3.13, 2014 edition);
- d) The term "timestamp mark" has been changed to "timestamp token" (see 3.15, 2014 edition of 3.15);
- e) Modified "Long-lasting signatures", "Timed CAAdES", "Archived CAAdES", "Content information", "Signature data", and "Signer information".

Definitions of the terms "information", "timestamping organization", "archiving timestamp", and "trust anchor" (see 3.1, 3.6~3.10, 3.14, 3.17, 3.18, 2014 edition).

(3.1, 3.6~3.10, 3.14, 3.17, 3.18)

- f) The term "CMS Advanced Electronic Signature" has been added (see 3.5);
- g) The term "CMS digital signature" has been removed (see 3.5 in the 2014 edition);
- h) Added a notation for requirement levels (see 6.2);

Additional methods defined in ISO 14533-4:2019 have been added (see 6.6, 6.7 and Annex B);

- j) Appendix A has been changed from normative to informative, and content related to ArchiveTimeStampV3 has been added (see Appendix A, 2014).

Appendix A of the 2017 edition).

This document is equivalent to ISO 14533-1:2022 "Long-term signatures of data elements, processes and documents in administration, commerce and industry - Part 1".

Part. CMS Advanced Digital Signature (CAAdES) Specification.

The following minimal editorial changes have been made to this document.

---The portion of the range is designated as "Note 1";

---Added a note for version 6.5.4.

Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying patents.

This document was proposed and is under the jurisdiction of the National Electronic Business Standardization Technical Committee (SAC/TC83).

Introduction

GB/T 31308 "Long-term signatures for data elements, processes and documents in administrative, commercial and industrial settings" is an interoperability standard to ensure the implementation of long-term signatures.

The standard for ensuring the long-term verifiability of electronic signatures is crucial for the security of the e-commerce market. GB/T 31308 is proposed to be jointly developed by four departments.

Composition.

---Part 1: CMS Advanced Digital Signature (CAAdES) Specification. The purpose is to clarify the CMS Advanced Digital Signature (CAAdES) specification.

The long-term signature standard ensures that this type of electronic signature can be verified over a long period of time.

---Part 2: XML, Advanced Digital Signatures (XAdES) Specification. The purpose is to clarify the XML Advanced Digital Signatures (XAdES) specification.

The long-term signature specification ensures that this type of electronic signature can be verified over a long period of time.

---Part 3: Long-lasting signature specifications for PDF Advanced Digital Signatures (PAdES). The purpose is to clarify the advanced digital signature (PAdES) specification for PDF.

The (PAdES) long-term signature specification ensures that this type of electronic signature can be verified over a long period of time.

---Part 4: Attributes of the Evidence Object Used for Long-Term Signature Formats. The purpose is to clarify the attributes of the evidence object required for long-term signature verification.

The specifications ensure that electronic signatures can be verified over a long period of time.

GB/T 31308 (all parts) are adopted one-to-one with ISO 14533 (all parts) to ensure the long-term verification of electronic signatures.

The implementation standards are aligned with international standards. By formulating this series of standards, the relevant standard system is improved.

The purpose of this document is to ensure interoperability between relevant implementations, particularly regarding long-term signatures, enabling digital signatures to last for extended periods.

The verification process is ongoing. Each reference implementation's long signature specification covers the Cryptographic Message Syntax (CMS) defined in IETF RFC 5652.

Digital signatures, including the CAAdES digital signature developed by the European Telecommunications Standards Institute (ETSI).

Data elements, processes, and... in administration, commerce, and industry document
Long-Term Signature Part 1: CMS Advanced Electronic Signature (CAAdES) Specification

1 Scope

This document specifies the digital signatures used for long-term verification as defined in CMS Advanced Electronic Digital Signatures and CAAdES Digital Signatures.

Data element.

This document applies to CAAdES long-term signing of data elements, processes, and documents in administrative, commercial, and industry settings.

Note 1: This document does not provide technical specifications for digital signatures themselves, nor does it restrict the use of existing digital signature specifications.

Note 2: CMS Advanced Digital Signatures (CAAdES) is an extension of the widely used Cryptographic Message Syntax (CMS).

2 Normative references

The contents of the following documents, through normative references within the text, constitute essential provisions of this document. Dated citations are not included.

For references to documents, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies.

This document.

ISO 14533-4 Long-term signatures for data elements, processes and documents in administration, commerce and industry - Part 4: Pointers to proof of existence Note. GB/T 31308.4-2023 Long-term signatures for data elements, processes and documents in administrative, commercial and industrial settings - Part 4: Formats for long-term signatures Attributes of the evidence-preserving object (ISO 14533-4:2019, IDT)