

ICS 35.240.60

CCS L 79



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

GB/T 31308.3-2023

**Processes, data elements and documents in commerce, industry and
administration - Long term signature - Part 3: Long term signature
profiles for PDF Advanced Electronic Signatures(PAdES)**

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

(English Translation)

Issued on: December 28, 2023

Implemented on: April 1, 2024

**Issued by: State Administration for Market Regulation, China National
Standardization Administration**

Table of Contents

Preface
Introduction
1 Scope
2 Normative references
3 Terms and Definitions
4 Symbols and abbreviations
5 Requirements
6 Long-term signature
Appendix A (Normative) Provider's Declaration of Conformity and its Attachments
Appendix B (Normative) Configuration files using only timestamps
Appendix C (Normative) Timestamp Token Structure
Appendix D (Informative) Applying PAdES via CMS Signature
Appendix E (informative) Example of multiple signatures
Reference

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 3 of GB/T 31308: GB/T 31308 has released the following parts:

- Specifications for long-lasting signatures of commercial, industrial and administrative processes, data elements and documents Part 1: CMS advanced electronic signatures (CAdES) long-term signature specification (GB/T 31308.1-2014);
- Specifications for long-term signatures of commercial, industrial and administrative processes, data elements and documents Part 2: XML advanced electronic signatures (XAdES) long-term signature specification (GB/T 31308.2-2014);
- Long-lasting signatures of data elements, processes and documents in administration, commerce and industry Part 3: PDF advanced electronic signatures
- Long-lasting signatures of data elements, processes and documents in administration, commerce and industry Part 4: Storage certificates for long-lasting signature formats Object attributes (GB/T 31308.4-2023):

This document is equivalent to ISO 14533-3:2017 "Long-term signature of data elements,

processes and documents in business, industry and administration Part 3" Part:
Long-lasting signature specification for PDF Advanced Electronic Signature (PAdES):

Introduction

GB/T 31308 is a standard that ensures the interoperability of long-term signatures and enables long-term verification of electronic signatures: For the e-commerce market Field security plays a major role: GB/T 31308 is planned to consist of 4 parts:

---Part 1: Long-term signature specification for CMS Advanced Electronic Signature (CAdES): The purpose is to clarify CMS advanced electronic signatures (CAdES) long-term signature specification ensures that this type of electronic signature can be verified for a long time:

---Part 2: Long-term signature specification for XML Advanced Electronic Signature (XAdES): The purpose is to clarify XML advanced electronic signatures (XAdES) long-term signature specification ensures that this type of electronic signature can be verified for a long time:

---Part 3: Long-lasting signature specifications for PDF Advanced Electronic Signature (PAdES): The purpose is to clarify PDF advanced electronic signatures (PAdES) long-term signature specification ensures that this type of electronic signature can be verified for a long time:

---Part 4: Attributes of the certificate object used in the long-lasting signature format: The purpose is to clarify the attributes of the certificate objects required for long-term signature verification:

Specific specifications to ensure that electronic signatures can be verified over the long term:

GB/T 31308 (all parts) adopts ISO 14533 (all parts) in one-to-one correspondence to ensure the long-term verification of electronic signatures:

Implementation standards are in line with international standards: By formulating this series of standards, the relevant standard system will be improved:

Data elements, processes and documents in administration, business and industry
Long-lasting signatures Part 3: PDF advanced electronic signatures (PAdES) long-term signature specification

1 Scope

This document specifies the relevant elements of PDF Advanced Electronic Signature (PAdES) to ensure that digital signatures can be verified in the long term:

This document does not give new technical specifications for digital signatures, nor does it

put forward new constraints on the use of existing digital signature technical specifications:

2 Normative reference documents

The contents of the following documents constitute essential provisions of this document through normative references in the text: Among them, the dated quotations for undated referenced documents, only the version corresponding to that date applies to this document; for undated referenced documents, the latest version (including all amendments) applies to this document:

ISO 14533-1 Specification for long-lasting signatures of processes, data elements and documents for commercial, industrial and administrative purposes Part 1: CMS Advanced Electronics (CAAdES)] Note: GB/T 31308.1-2014 Specification for long-term signature of commercial, industrial and administrative processes, data elements and documents Part 1: CMS advanced electronic signature Card signature specification (ISO 14533-1:2012, IDT) named (CAAdES):

3 Terms and definitions

The terms and definitions defined in ISO 14533-1 and the following apply to this document:

An electronic signature that is uniquely associated with and identifies the signer: It is created using electronic signature data and can detect for all changes, the signer can be sure that he is the only person who can control the electronic signature:

4 Symbols and abbreviations

The following symbols and abbreviations apply to this document:

C: conditional

M: Essential

O: optional

P: Prohibited type (create or modify)