

ICS 35.240.60
CCS L 79



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

GB/T 31308.4-2023

**Processes, data elements and documents in commerce, industry and
administration - Long term signature - Part 4: Attributes pointing to
proof of existence objects used in long term signature formats**

行政、商业和行业中的数据元、过程和文档 长效签名 第4部分：用于长效签名格
式的存证对象属性

(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 PoE attributes
5 Types of PoE objects and their basic fields
Appendix A (Normative) ASN:1 Module
Appendix C (Normative) Signature timestamps as timestamps via OCSP
Appendix D (Normative) Syntax for ASN:1 object positions in ZIP, PDF containers or DER encoded ASN:1 objects
Appendix E (normative) Usage of PoE (proof of possession) objects
Appendix F (informative) Position of DTId in digital signature
Appendix G (informative) Media type registration
Appendix H (Informative) Evidence Record Syntax Object
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 4 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 (CAAdES) 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 (PAdES) long-term signature specification (GB/T 31308.3-2023);
- Long-lasting signatures of data elements, processes and documents in administration,

commerce and industry Part 4: Storage certificates for long-lasting signature formats this document is equivalent to ISO 14533-4:2019 "Specification for long-term signatures of data elements, processes and documents in administration, commerce and industry" Part 4: Attestation object attributes for long-lasting signature formats:

This document has made the following minimal editorial changes:

---Change the name of the standard to "Long-term signature of data elements, processes and documents in administration, commerce and industry - Part 4: For long-term signatures" Name format of the certificate object attribute:

Please note that some content in this document may be subject to patents: The publisher of this document assumes no responsibility for identifying patents:

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 (CAAdES): The purpose is to clarify CMS advanced electronic signatures (CAAdES) 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 4: Format for long-lasting signatures Certificate object
properties

1 Scope

This document specifies the PoE (Proof of Existence) attributes and objects used in the long-term signature format, and describes the basic concept of PoE:

Concepts and attribute characteristics are given, and the types, basic fields, and related examples of PoE objects are given:

This document applies to (external) certificate objects used in long-lasting signature formats, i.e. through existing available digital signatures and trusted times:

The value implements dynamic verification of long-lasting signatures:

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:

Note: GB/T 16263.1-2006 Information technology ASN.1 encoding rules Part 1: Basic encoding rules (BER), regular encoding rules (CER) and Atypical Encoding Rules (DER) Specification (ISO/IEC 8825-1:2002, IDT) ISO/IEC 9594-8 Information technology open systems interconnection catalog Part 8: Public key and attribute certificate framework Note: GB/T 16264.8-2005 Information technology open system interconnection catalog Part 8: Public key and attribute certificate framework (ISO/IEC 9594-8:

2001, IDT)

ETSI EN 319122-1 V1.1.1:2016 Electronic Signatures and Infrastructure (ESI) CAdES (CMS Advanced Electronic Signature, CMS line signatures]

1) See <https://tools.ietf.org/html/3161>: