Chinastandards.org

ICS 35.030
CCS L 80

GM

GM/T 0125.1-2022

JavaScript Object Notation Web cryptographic application syntax specification-Part 1:Algorithm identifier

JSON Web 密码应用语法规范 第1部分：算法标识

(English Translation)

Issued on: November 20, 2022 **Implemented on: June 1, 2023**

Issued by: State Administration of Cryptography

Preview: page 1 of 3 shown, 7 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0125-1-2022

Chinastandards.org

Table of Contents

Foreword 1
Scope 2
Normative References 3
Terms and Definitions 4
JSON Javascript Object Notation 5
Abbreviations 6

Foreword

This document was drafted in accordance with the rules provided in GB/T 1.1-2020 Directives for Standardization - Part 1: Rules for the Structure and Drafting of Standardizing Documents.

This document is Part 1 of GM/T 0125 JavaScript Object Notation Web Cryptographic Application Syntax Specification. GM/T 0125 has issued the following parts.

---Part 1: Algorithm Identifier;

---Part 2: Signature;

---Part 3: Data Encryption;

---Part 4: Key.

Please be noted that certain content of this document may involve patents. The institution issuing this document does not undertake the responsibility of identifying these patents.

This document was proposed by and shall be under the jurisdiction of Cryptography Standardization Technical Committee.

1 Scope

This document defines the algorithm identifier of JSON Web cryptographic applications.

This document is applicable to the research and development and testing of JSON Web cryptographic application products. It can be used as a reference for other security products that use the JSON data exchange format.

Preview: page 2 of 3 shown, 7 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0125-1-2022

2 Normative References

The contents of the following documents constitute indispensable clauses of this document through the normative references in the text. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GM/T 0006 Cryptographic Application Identifier Criterion Specification GM/Z 4001 Cryptology Terminology

3 Terms and Definitions

The terms and definitions defined in GM/Z 4001 and the following are applicable to this document.

3.1 JSON Javascript Object Notation

JavaScript object notation, a lightweight, text-based, language-independent data exchange format.

4 Abbreviations

The following abbreviations apply to this document.

CCM. Counter with Cipher Block Chaining-Message Authentication Code GCM. Galois/Counter Mode .....

Preview: page 3 of 3 shown, 7 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0125-1-2022