

ICS 35.040
CCS L 80



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

GB/T 32918.3-2016

**Information security technology-Public key cryptographic
algorithm SM2 based on elliptic curves-Part 3: Key exchange
protocol**

信息安全技术 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议

Issued on: August 29, 2016

Implemented on: March 1, 2017

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

Foreword

1 Scope

2 Normative references

3 Terms and definitions

About this edition

Edition history and citation

Classification and status

How a Chinese national standard is set out

What is delivered

How this standard is designated

Foreword

This document was issued on 29 August 2016 by the State Administration for Market Regulation and the Standardization Administration of the People's Republic of China, and has been in force since 1 March 2017.

It is the first edition of this standard.

The document is under the responsibility of the Standardization Administration of China.

Classification: ICS 35.040, CCS L 80.

1 Scope

GB/T 32918.3-2016 is the Chinese national standard covering information security technology, Public key cryptographic algorithm SM2 based on elliptic curves, Part 3: Key exchange protocol. It was issued on 29 August 2016 and has been in force since 1 March 2017, as a first edition. The document is under the responsibility of the Standardization Administration of China. This page is published from the official record of the 2016 edition. The figures, limits and tables the standard contains are those of the document itself, delivered in full with the English translation.

2 Normative references

Clause 2 of GB/T 32918.3-2016 lists the normative references: the other standards that have to be applied together with this one for its requirements to be met. A dated reference means that only that edition applies; an undated one means the latest edition applies,

amendments included.

These references are part of the requirements, not a reading list. A laboratory or an inspection body working to GB/T 32918.3-2016 needs the referenced documents in hand, and a specification that cites GB/T 32918.3-2016 inherits them. The list is printed in the standard itself.

3 Terms and definitions

Clause 3 of GB/T 32918.3-2016 gives the terms and definitions that apply to the document. In a Chinese national standard a definition is either written out in full or taken from another standard, and in that case the source is printed in square brackets after it, so that the same term keeps one meaning across the whole family of standards that use it.

The definitions decide how the requirements are read: two documents can use the same word for different things, and clause 3 is where the standard says which one it means. The terms are printed in the standard itself, with the Chinese alongside the English.

About this edition

GB/T 32918.3-2016 is the first edition of this standard. It was issued on 29 August 2016 and has been in force since 1 March 2017.

There is no earlier edition to compare it with, so a specification that has to refer to this subject can only cite GB/T 32918.3-2016 itself.

The interval between issue and effect is the transition period. It exists so that producers, laboratories and buyers can requalify products, revise procedures and use up documentation before the new text becomes the one that applies. The date on this page is the official one from the record of the Standardization Administration.

Edition history and citation

GB/T 32918.3-2016 is a first edition: there is no earlier version of this standard, so a document that needs to refer to this subject can only cite GB/T 32918.3-2016 itself.

Where an edition is replaced, the Chinese standardization system keeps the number and changes the year: the number identifies the subject, the year identifies the text. That is why a citation without a year is ambiguous and a citation with one is not.

Classification and status

GB/T 32918.3-2016 is classified under ICS 35.040, in the field of information technology. ICS is the International Classification for Standards, the same scheme used by ISO and by the national bodies of most countries, which is what allows a Chinese standard to be

placed beside its foreign counterparts on subject rather than on number.

Its Chinese Standard Classification code is CCS L 80. CCS is the domestic scheme, a letter for the sector and two digits for the subject within it, and it is the code by which the standard is filed and searched in China.

The GB/T prefix marks a recommended national standard. It is not, in itself, law: it becomes binding when a contract names it, when a regulation or a mandatory standard refers to it, or when a producer declares conformity with it. In practice that covers most of the cases in which it will be read - a purchase specification, an inspection agreement or a certification scheme.

The document is under the responsibility of the Standardization Administration of China, which is the body that maintains it and that will answer a formal question about its interpretation.

How a Chinese national standard is set out

Chinese national standards are drafted to the rules of GB/T 1.1, which fixes the order in which a standard is set out. The same order is used by every GB standard, so a reader who knows one knows where to look in any other:

Foreword - the issuing bodies, the relationship to any previous edition, the technical committee responsible for the document, and the list of the organisations that drafted it.

1 Scope - what the document covers and what it does not, and the products, activities or materials it applies to.

2 Normative references - the other standards that have to be applied together with this one. A dated reference means that edition only; an undated one means the latest edition, amendments included.

3 Terms and definitions - the vocabulary that decides how the requirements are read. Definitions are either written out or taken from another standard, with the source printed after them.

4 and onwards, the technical clauses - the requirements themselves, then the test or measurement methods by which conformity is established, then the inspection rules that say how a lot is sampled and judged, and, for a product standard, the provisions on marking, packaging, transport and storage. How many clauses there are, and how they are divided into subclauses, depends on the document.

Annexes - normative when they carry requirements, informative when they carry guidance, lettered A, B, C in the order they are first cited in the text.

Bibliography - the documents referred to for information only, which are not part of the requirements.

The numbering of the clauses and subclauses of GB/T 32918.3-2016, and the text under each of them, are in the standard itself: they are delivered in full with the English translation.

What is delivered is the complete document in that order: every clause, every table, every figure and every annex of the Chinese original, with the same numbering, so that a reference to a clause number in a contract or a test report points to the same place in both languages.

What is delivered

The English edition of GB/T 32918.3-2016 is delivered as a complete PDF of the whole standard - every clause, table, figure and annex - not an extract or a summary.

Clause and subclause numbers, table and figure numbers and annex letters are those of the Chinese original, so a reference to a clause in a contract, a purchase specification or a test report points to the same place in both languages.

Quantities, units and symbols are carried over unchanged. Chinese standards use SI, so a limit read from the English text is the limit a Chinese inspection body applies reading the Chinese one.

How this standard is designated

The full designation is GB/T 32918.3-2016. A citation should carry the number with its year, because the year identifies the text that applies.

In a catalogue or a filing system it is found under ICS 35.040 and CCS L 80 - the international classification and the Chinese one, which are the two codes by which a standard on this subject is searched.