

INTERNATIONAL STANDARD

ISO
11166-2

First edition
1994-11-15

ANSI Internat Doc Sec

Banking — Key management by means of asymmetric algorithms —

Part 2:

Approved algorithms using the RSA
cryptosystem

*Banque — Gestion des clés au moyen d'algorithmes asymétriques —
Partie 2: Algorithmes approuvés utilisant le système de chiffrement RSA*



Reference number
ISO 11166-2:1994(E)
AVA Documents
Document Sharing Hub

Contents

	Page
Introduction	i v
1 Scope	1
2 Normative references	1
3 Definitions and notation	1
4 Symbols and abbreviations	1
5 RSA key generation	2
6 RSA encipherment and decipherment	2
7 Modes of operation for RSA signature	2
8 Application of algorithms	4
Annexes	
A Assigned values of Function and Format Code (FFC)	7
B Choice of primes	10
C Bibliography	12

© ISO 1994

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Organization for Standardization
Case Postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

Draft International Standards adopted by the technical committees are circulated to the member bodies for approval before their acceptance as International Standards by the ISO Council. They are approved in accordance with ISO procedures requiring at least 75% approval by the member bodies voting.

International Standard ISO 11166-2 was prepared by Technical Committee ISO/TC 68, *Banking and relating financial services*, Subcommittee 2, *Operations and procedures*.

ISO 11166 consists of the following parts, under the general title *Banking — Key management by means of asymmetric algorithms*:

— *Part 1: Principles, procedures and formats*

— *Part 2: Approved algorithms using the RSA cryptosystem.*

Annex A forms an integral part of this part of ISO 11166. Annexes B and C are for information only.

Introduction

ISO 11166-1 specifies those aspects of banking key management using asymmetric algorithms which are independent of the algorithms employed. Subsequent parts of the standard specify asymmetric algorithms which are approved for use in the procedures of part 1.

This part of ISO 11166 specifies approved algorithms using the RSA cryptosystem. It also provides a link between the algorithm specification and the notation used in part 1 to denote the primitive cryptographic processes employed in banking key management.

It is envisaged that alternative approved algorithms will be specified in further parts of the standard, no single algorithm being mandatory.

The level of security achievable by the use of a cryptographic algorithm depends, among other factors, on parameters defining the algorithm and on the current state of information processing technology. Because of these dependencies, no specific level of security is implied by the general approval of an algorithm for use in part 1 procedures.

Annex A specifies the assigned values of the Format and Function Code (FFC) to be used when certificates are signed by transforming the text.

Banking — Key management by means of asymmetric algorithms —

Part 2:

Approved algorithms using the RSA cryptosystem

1 Scope

This part of ISO 11166 specifies asymmetric algorithms, i.e. algorithms for asymmetric encipherment and digital signature, employing the RSA cryptosystem and approved for use with ISO 11166-1.

This part of ISO 11166 specifies particular uses of the RSA method. It does not describe the RSA cryptosystem in its general form. Modes of operation for RSA digital signature are also specified. These algorithms and modes of operation are for use only in part 1 of this International Standard.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 11166. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO 11166 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 646:1991, *Information technology — ISO 7-bit coded character set for information interchange*.

ISO 9362:-¹⁾, *Banking — Banking telecommunication messages — Bank identifier codes*.

ISO 11166-1:1994, *Banking — Key management by means of asymmetric algorithms — Part 1: Principles, protocols and formats*.

3 Definitions and notation

The definitions given in ISO 11166-1, along with the following, apply.

3.1 extended public key : That part of the asymmetric key set which is employed for encipherment and for signature deconstruction.

3.2 extended secret key : That part of the asymmetric key set which is employed for decipherment and for signature construction.

3.3 hash function : A mathematical function operating on a text of indefinite length with a result of fixed length, which has the property that it is computationally unfeasible to produce two texts giving the same result.

3.4 hash result : The result of applying a hash function. In this part of ISO 11166 the hash result is represented by a non-negative integer.

The notation given in ISO 11166-1 for encipherment, decipherment, signature construction and signature deconstruction shall apply. The notation is extended in this part of ISO 11166 to enable a mathematical formulation of these functions to be specified.

4 Symbols and abbreviations

n Size of modulus, in bits

M Modulus

NOTE — The abbreviation "mod M " signifies that the result of an arithmetic operation shall be replaced by its least non-negative residue, modulo M .

X Text for encipherment

Y Enciphered text

T Text for signature

h Hash function

H Hash result

S Digital signature

E Public exponent

D Secret exponent

¹⁾To be published (Revision of ISO 9362:1987)

KS1	Extended secret key of the sender of a KSM
KS2	Extended secret key of the receiver of a KSM
KP1	Extended public key of the sender of a KSM
KP2	Extended public key of the receiver of a KSM
P, Q	Prime numbers, whose product is M
lcm	Lowest common multiple
TR	Text recovery, a signature mode of operation
TH	Text hashing, a signature mode of operation

5 RSA key generation

The values of n , the size of modulus, and E , the public exponent, shall be fixed parameters, to be agreed for each application of RSA key sets.

NOTE — It is recommended that n be a multiple of 8. For rapid encipherment and signature verification, a convenient value is $E = 65\,537$ which rarely restricts the choice of the primes. Where different RSA key sets are used for different purposes (such as encipherment and signature in KSMs and signature in certificates) the key sets for each purpose may have their own parameter values n and E .

Two primes P and Q shall be found, such that their product, which is the modulus M , satisfies the inequalities :

$$2^{n-1} < M = PQ < 2^n$$

The primes P and Q shall be chosen independently by random processes such that there is no number with a greater than 2^{-64} probability of being chosen for P and Q .

Methods of testing and finding primes and of calculating D are not part of this part of ISO 11166. "Probable primes" obtained by primality testing may be used, provided that the probability of choosing a composite number is less than 2^{-30} .

The chosen values of P and Q shall be such that $P-1$ and $Q-1$ are each relatively prime to E .

All intermediate values employed in finding primes P and Q and the primes themselves shall be treated as secret values with the same level of security as a secret cryptographic key, in accordance with ISO 11166-1:1994, clauses 1.6 and 1.7.

Secret exponent D shall be the least positive solution of :

$$ED = 1 \bmod \text{lcm}(P-1, Q-1)$$

Exponent D shall be treated as a secret value with the same level of security as a secret cryptographic key, in accordance with ISO 11666-1:1994, clauses 1.6 and 1.7.

When $M = PQ$ and secret exponent D have been calculated, all intermediate values shall be destroyed unless a method of computation is to be employed which requires P or Q or values derived therefrom to be retained as secret values. Annex B describes some conditions on P and Q that have been proposed.

The extended secret key comprises the numbers D and M . The extended public key comprises the numbers E and M .

6 RSA encipherment and decipherment

6.1 Encipherment

The text for encipherment shall be expressed as a non-negative integer X which is less than M .

Encipherment shall be the result of the following calculation :

$$Y = X^E \bmod M$$

The result of encipherment is expressed as an integer Y .

6.2 Decipherment

The enciphered text shall be expressed as an integer Y which is less than M .

Decipherment shall be the result of the following calculation :

$$X = Y^D \bmod M$$

The result of decipherment is expressed as an integer X .

7 Modes of operation for RSA signature

7.1 Text recovery mode of operation (TR)

Figure 1 shows schematically the text recovery mode of operation.

This mode of operation for RSA is an example of signature construction by transforming the text, as specified in ISO 11166-1:1994, subclause 3.3.1.2.(a).

The text recovery mode of operation may only be applied to a block of text represented by an integer T which is less than M .