INTERNATIONAL STANDARD

ISO/IEC 9796-3

Second edition
2006-09-15

Information technology — Security techniques — Digital signature schemes giving message recovery —

Part 3: Discrete logarithm based mechanisms

Technologies de l'information — Techniques des sécurité — Schémas de signature numérique rétablissant le message —

Partie 3: Mécanismes basés sur les logarithmes discrets

Reference number
ISO/IEC 9796-3:2006(E)

© ISO/IEC 2006

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2006

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 either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols, notation and conventions 4
4.1 Symbols and notation 4
4.2 Conversion functions and mask generation functions 6
4.3 Legend for figures 6

5 Binding between signature mechanisms and hash-functions 7

6 Framework for digital signatures giving message recovery 7
6.1 Processes 7
6.2 Parameter generation process 8
6.3 Signature generation process 8
6.4 Signature verification process 9

7 General model for digital signatures giving message recovery 9
7.1 Requirements 9
7.2 Summary of functions and procedures 10
7.3 User key generation process 11
7.4 Signature generation process 11
7.5 Signature verification process 14

8 NR (Nyberg-Rueppel message recovery signature) 17
8.1 Domain parameter and user keys 17
8.2 Signature generation process 17
8.3 Signature verification process 18

9 ECNR (Elliptic Curve Nyberg-Rueppel message recovery signature) 19
9.1 Domain parameter and user keys 19
9.2 Signature generation process 19
9.3 Signature verification process 20

10 ECMR (Elliptic Curve Miyaji message recovery signature) 21
10.1 Domain parameter and user keys 21
10.2 Signature generation process 22
10.3 Signature verification process 23

11 ECAO (Elliptic Curve Abe-Okamoto message recovery signature) 23
11.1 Domain parameter 23
11.2 User keys 24
11.3 Signature generation process 24
11.4 Signature verification process 26

12 ECPV (Elliptic Curve Pintsov-Vanstone message recovery signature) 27
12.1 Domain and user parameters 27
12.2 Signature generation process 28
12.3 Signature verification process 29

13 ECKNR (Elliptic Curve KCDSA/Nyberg-Rueppel message recovery signature) 31
13.1 Domain parameter and user keys 31
13.2 Signature generation process 31
13.3 Signature verification process 32

© ISO/IEC 2006 – All rights reserved

Annex A (informative) **Mathematical conventions** **34**
A.1 Bit strings **34**
A.2 Octet strings **34**
A.3 Finite fields **34**
A.4 Elliptic curves **35**

Annex B (normative) **Conversion functions** **36**
B.1 Octet string / bit string conversion: OS2BSP and BS2OSP **36**
B.2 Bit string / integer conversion: BS2IP and I2BSP **36**
B.3 Octet string / integer conversion: OS2IP and I2OSP **36**
B.4 Finite field element / integer conversion: FE2IP$_F$ **36**
B.5 Octet string / finite field element conversion: OS2FEP$_F$ and FE2OSP$_F$ **37**
B.6 Elliptic curve / octet string conversion: EC2OSP$_E$ and OS2ECP$_E$ **37**

Annex C (normative) **Mask generation functions (Key derivation functions)** **39**
C.1 Allowable mask generation functions **39**
C.2 MGF1 ..... **39**
C.3 MGF2 ..... **39**

Annex D (informative) **Example method for producing the data input** **40**
D.1 Splitting the message and producing the data input **40**
D.2 Checking the redundancy **40**

Annex E (normative) **ASN.1 module** **42**
E.1 Formal definition **42**
E.2 Use of subsequent object identifiers **43**

Annex F (informative) **Numerical examples** **44**
F.1 Numerical examples for NR **44**
F.2 Numerical examples for ECNR **47**
F.3 Numerical examples for ECMR **51**
F.4 Numerical examples for ECAO **54**
F.5 Numerical examples for ECPV **59**
F.6 Numerical examples for ECKNR **62**

Annex G (informative) **Summary of properties of mechanisms** **66**

Annex H (informative) **Correspondence of schemes** **68**

Bibliography **69**

 © ISO/IEC 2006 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

ISO/IEC 9796-3 was prepared by Joint Technical Committee ISO/IEC /JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 9796-3:2000), which has been technically revised. New mechanisms and object identifiers have been specified.

ISO/IEC 9796 consists of the following parts, under the general title *Information technology — Security techniques — Digital signature schemes giving message recovery*:

— *Part 2: Integer factorization based mechanisms*

— *Part 3: Discrete logarithm based mechanisms*

© ISO/IEC 2006 – All rights reserved

Introduction

Digital signature mechanisms can be used to provide services such as entity authentication, data origin authentication, non-repudiation, and integrity of data.

A digital signature mechanism satisfies the following requirements:

— given only the public verification key and not the private signature key, it is computationally infeasible to produce a valid signature for any given message;

— the signatures produced by a signer can neither be used for producing a valid signature for any new message nor for recovering the signature key;

— it is computationally infeasible, even for the signer, to find two different messages with the same signature.

Most digital signature mechanisms are based on asymmetric cryptographic techniques and involve three basic operations:

— a process for generating pairs of keys, where each pair consists of a private signature key and the corresponding public verification key;

— a process using the private signature key, called the ***signature generation process***;

— a process using the public verification key, called the ***signature verification process***.

There are two types of digital signature mechanisms:

— when, for each given private signature key, the signatures produced for the same message are the same, the mechanism is said to be ***non-randomized*** (or ***deterministic***) [see ISO/IEC 14888-1];

— when, for a given message and a given private signature key, each application of the signature process produces a different signature, the mechanism is said to be ***randomized***.

This part of ISO/IEC 9796 specifies randomized mechanisms.

Digital signature schemes can also be divided into the following two categories:

— when the whole message has to be stored and/or transmitted along with the signature, the mechanism is named a ***signature mechanism with appendix*** [see ISO/IEC 14888];

— when the whole message or a part of it is recovered from the signature, the mechanism is named a ***signature mechanism giving message recovery***.

If the message is short enough, then the entire message can be included in the signature, and recovered from the signature in the signature verification process. Otherwise, a part of the message can be included in the signature and the rest of it is stored and/or transmitted along with the signature. The mechanisms specified in ISO/IEC 9796 give either total or partial recovery, aiming at reducing storage and transmission overhead.

This part of ISO/IEC 9796 includes six mechanisms, one of which was in ISO/IEC 9796-3:2000 and five of which are in ISO/IEC 15946-4:2004. The mechanisms specified in this part of ISO/IEC 9796 use a hash-function to hash the entire message. ISO/IEC 10118 specifies hash-functions. Some of the mechanisms specified in this part of ISO/IEC 9796 use a group on an elliptic curve over finite field. ISO/IEC 15946-1:2002 describes the mathematical background and general techniques necessary for implementing cryptosystems based on elliptic curves defined over finite fields.

 © ISO/IEC 2006 – All rights reserved

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the mechanisms NR, ECMR and ECAO given in Clause 8, 10 and 11, respectively.

Area	Patent no.	Issue date	Inventors
NR [see Clause 8]	US 5 600 725, EP 0 639 907	1997-02-04	K. Nyberg and R. A. Rueppel
ECMR [see Clause 10]	JP H09-160492 (patent application)		A. Miyaji
ECAO [see Clause 11]	JP 3 434 251	2003-08-04	M. Abe and T. Okamoto

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured the ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holders of these patent rights are registered with ISO and IEC. Information may be obtained from the following companies.

Patent no.	Name of holder of patent right	Contact address
US 5 600 725, EP 0 639 907	Certicom Corp.	5520 Explorer Drive, 4th Floor, Mississauga, Ontario, Canada L4W 5L1
JP H09-160492	Matsushita Electric Industrial Co., Ltd.	Matsushita IMP Building 19th Floor, 1-3-7, Siromi, Chuo-ku, Osaka 540-6319, Japan
JP 3 434 251	NTT Intellectual Property Center	9-11 Midori-Cho 3-chome, Musashino-shi, Tokyo 180-8585, Japan

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

NOTE 1 Computational feasibility depends on the specific security requirements and environment.

NOTE 2 Any signature mechanism giving message recovery — for example, the mechanisms specified in this part of ISO/IEC 9796 — can be converted for provision of digital signatures with appendix. In this case, the signature is produced by application of the signature mechanism to a hash-token of the message.

© ISO/IEC 2006 – All rights reserved

Information technology — Security techniques — Digital signature schemes giving message recovery —

Part 3: Discrete logarithm based mechanisms

1 Scope

This part of ISO/IEC 9796 specifies six digital signature schemes giving message recovery. The security of these schemes is based on the difficulty of the discrete logarithm problem, which is defined on a finite field or an elliptic curve over a finite field.

This part of ISO/IEC 9796 also defines an optional control field in the hash-token, which can provide added security to the signature.

This part of ISO/IEC 9796 specifies randomized mechanisms.

The mechanisms specified in this part of ISO/IEC 9796 give either total or partial message recovery.

NOTE For discrete logarithm based digital signature schemes with appendix, see ISO/IEC 14888-3.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*

ISO/IEC 15946-1:2002, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General*

© ISO/IEC 2006 – All rights reserved