INTERNATIONAL STANDARD

ISO/IEC 9796-3

Second edition
2006-09-15

Corrected version
2013-09-15

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)

Documents
Document Sharing Hub
© ISO/IEC 2006

Full document details: ISO IEC 09796-3-2006 (2013)

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

© ISO/IEC 2006 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO IEC 09796-3-2006 (2013)

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

Documents
Document Sharing Hub

© ISO/IEC 2006 – All rights reserved

Full document details: ISO IEC 09796-3-2006 (2013)

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

Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

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*

This corrected version of ISO/IEC 9796-3:2006 incorporates the following corrections:

— The year of publication has been removed from references to ISO/IEC 15946-1.

— The last paragraph of 6.2.1 has been modified and ISO/IEC 15946-5 has been added to Clause 2.

© ISO/IEC 2006 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

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 describes the mathematical background and general techniques necessary for implementing cryptosystems based on elliptic curves defined over finite fields.

Documents
Document Sharing Hub

© ISO/IEC 2006 – All rights reserved

Full document details: ISO IEC 09796-3-2006 (2013)

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

Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

Documents
Document Sharing Hub

Full document details: ISO IEC 09796-3-2006 (2013)

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, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General*

ISO/IEC 15946-5, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
data input
octet string which depends on the entire message or a portion of the message and which forms a part of the input to the signature generation process

3.2
domain parameter
data item which is common to and known by or accessible to all entities within the domain

[ISO/IEC 14888-1:1998]

© ISO/IEC 2006 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

NOTE The set of domain parameters may contain data items such as hash-function identifier, length of the hash-token, maximum length of the recoverable part of the message, finite field parameters, elliptic curve parameters, or other parameters specifying the security policy in the domain.

3.3
elliptic curve
set of points $P = (x, y)$, where x and y are elements of an explicitly given finite field, that satisfy a cubic equation without any singular point, together with the "point at infinity" denoted by $\circ$

[ISO/IEC 15946-1:2002]

NOTE For a mathematical definition of an elliptic curve over an explicitly given finite field, see Clause A.4.

3.4
explicitly given finite field
set of all e-tuples over $[0, p-1]$, where p is prime and $e \geq 1$, along with a "multiplication table"

NOTE 1 For a mathematical definition of an explicitly given finite field, see Clause A.3.

NOTE 2 For more detailed information on finite fields, see ISO/IEC 15946-1.

3.5
hash-code
string of octets which is the output of a hash-function

NOTE Adapted from ISO/IEC 10118-1:2000.

3.6
hash-function
function which maps strings of octets to fixed-length strings of octets, satisfying the following two properties:

— for a given output, it is computationally infeasible to find an input which maps to this output;

— for a given input, it is computationally infeasible to find a second input which maps to the same output.

NOTE 1 Adapted from ISO/IEC 10118-1:2000.

NOTE 2 Computational feasibility depends on the specific security requirements and environment.

NOTE 3 For the purposes of this part of ISO/IEC 9796, the allowable hash-functions are those described in ISO/IEC 10118-2 and ISO/IEC 10118-3, with the following proviso:

— The hash-functions described in ISO/IEC 10118 map bit strings to bit strings, whereas in this part of ISO/IEC 9796, they map octet strings to octet strings. Therefore, a hash-function in ISO/IEC 10118-2 or ISO/IEC 10118-3 is allowed in this part of ISO/IEC 9796 only if the length in bits of the output is a multiple of 8, in which case the mapping between octet strings and bit strings is affected by the functions OS2BSP and BS2OSP.

3.7
hash-token
concatenation of a hash-code and an optional control field which can be used to identify the hash-function and the padding method

[ISO/IEC 14888-1:1998]

NOTE The control field with the hash-function identifier is mandatory unless the hash-function is uniquely determined by the signature mechanism or by the domain parameters.

3.8
message
string of octets of any length

3.9
parameter generation process
process which gives as its output domain parameter and user keys

© ISO/IEC 2006 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

3.10
pre-signature
octet string computed in the signature generation process which is a function of the randomizer but which is independent of the message

NOTE Adapted from ISO/IEC 14888-1:1998.

3.11
private signature key
data item specific to an entity and usable only by this entity in the signature generation process

3.12
public verification key
data item which is mathematically related to a private signature key and is known by or accessible to all entities and which is used by the verifier in the signature verification process

3.13
randomized
dependent on a randomizer

[ISO/IEC 14888-1]

3.14
randomizer
secret integer produced by the signing entity in the pre-signature production process, and not predictable by other entities

NOTE Adapted from ISO/IEC 14888-1:1998.

3.15
signature
pair of an octet string and an integer for providing authentication, generated in the signature generation process

NOTE Adapted from ISO/IEC 14888-1:1998.

3.16
signature generation process
process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature

NOTE Adapted from the definition of **signature process** in ISO/IEC 14888-1:1998.

3.17
signature verification process
process, which takes as its input the signed message, the verification key and the domain parameters, and which gives as its output the recovered message if valid

NOTE Adapted from the definition of **verification process** in ISO/IEC 14888-1:2008.

3.18
signed message
set of data items consisting of the signature, the part of the message which cannot be recovered from the signature, and an optional text field

[ISO/IEC 14888-1:1998]

3.19
user keys
data item of a set of private signature key and public verification key

© ISO/IEC 2006 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

4 Symbols, notation and conventions

4.1 Symbols and notation

For the purposes of this document, the following symbols and notation apply.

A	entity, usually signer
B	entity, usually verifier
d	data input (octet string)
d'	recovered data input (octet string)
E	elliptic curve over explicitly given finite field
F	explicitly given finite field
G	generator of underlying group (finite field element / elliptic curve point)
h	(truncated) hash-token (octet string)
h'	recovered (truncated) hash-token (octet string)
h''	recomputed (truncated) hash-token (octet string)
Hash, Hash_1, Hash_2	hash-function
k	randomizer (integer)
KDF	key derivation function (synonym for MGF)
L_{clr}	length in octets of non-recoverable part (integer)
L_{dat}	length in octets of data input (integer)
L_F	length in octets of explicitly given finite field F (non-negative integer)
L_{rec}	(maximum) length in octets of recoverable part (integer)
L_{red}	length in octets of (added) redundancy (integer)
$L(x)$	length in octets of integer x or octet string x (non-negative integer)
L_{Hash}	length in octets of output of hash-function Hash (non-negative integer)
M	message (octet string)
M_{clr}	non-recoverable part of message (octet string)
M_{rec}	recoverable part of message (octet string)
M'	recovered message (octet string)
M'_{clr}	received non-recoverable part of message (octet string)
M'_{rec}	recovered part of message (octet string)
MGF	mask generation function
n	order of group generated by G (prime number)

© ISO/IEC 2006 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

O	point at infinity of elliptic curve
p	prime number
P	element dependent on the chosen key generation scheme, that is $P = G$ for Key Generation Scheme I and $P = Y_A$ for Key Generation Scheme II [see Clause 7.3]
Π	pre-signature (octet string)
Π'	recovered pre-signature (octet string)
q	prime power
Q	element dependent on the chosen key generation scheme, that is $Q = Y_A$ for Key Generation Scheme I and $Q = G$ for Key Generation Scheme II [see Clause 7.3]
r	first part of signature (octet string)
r'	first part of recovered signature (octet string)
s	second part of signature (integer)
s'	second part of recovered signature (integer)
x_A	private signature key of entity A
Y_A	public verification key of entity A
$\{0, 1\}^*$	set of finite bit strings
$\{0, 1\}^{8*}$	set of finite octet strings
$\{0, 1\}^{\ell}$	set of bit strings of length ℓ, where ℓ is a non-negative integer
$\{0, 1\}^{8\ell}$	set of octet strings of length ℓ, where ℓ is a non-negative integer
$[a, b]$	set of integers x satisfying $a \le x \le b$, where a and b are integers
$\lvert x \rvert$	length of bit string x
$\lvert X \rvert$	cardinality of set X
$[x]^{\ell}$	leftmost ℓ-bits of octet string x, appending zeros to the right when $8\ell > L(x)$
$[x]_{\ell}$	rightmost ℓ-bits of octet string x, appending zeros to the left when $8\ell > L(x)$
$x \bmod n$	$r \in [0, n-1]$ such that $(x - r)$ is divisible by n, where x is an integer
$x \oplus y$	bitwise exclusive-OR operation of bit strings x and y
$x \lVert y$	concatenation of bit strings x and y
$X \times Y$	Cartesian product of sets X and Y

© ISO/IEC 2006 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

4.2 Conversion functions and mask generation functions

For the purposes of this document, the following conversion functions and mask generation functions are used.

BS2IP	bit-string-to-integer primitive [see Clause B.2]
BS2OSP	bit-string-to-octet-string primitive [see Clause B.1]
EC2OSP	elliptic-curve-to-octet-string primitive [see Clause B.6]
FE2IP	finite-field-element-to-integer primitive [see Clause B.4]
FE2OSP	finite-field-element-to-octet-string primitive [see Clause B.5]
I2BSP	integer-to-bit-string primitive [see Clause B.2]
I2OSP	integer-to-octet-string primitive [see Clause B.3]
MGF1	mask generation function 1 [see Clause C.2]
MGF2	mask generation function 2 [see Clause C.3]
OS2BSP	octet-string-to-bit-string primitive [see Clause B.1]
OS2ECP	octet-string-to-elliptic-curve primitive [see Clause B.6]
OS2FEP	octet-string-to-finite-field-element primitive [see Clause B.5]
OS2IP	octet-string-to-integer primitive [see Clause B.3]

4.3 Legend for figures

The following legend is used for the figures in Clause 7 depicting the signature generation and verification processes for digital signatures giving message recovery.

STEP OF THE PROCESS	step of the process
⟶	mandatory data flow
⇢	optional data flow

© ISO/IEC 2006 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

5 Binding between signature mechanisms and hash-functions

Use of the signature schemes specified in this part of ISO/IEC 9796 requires the selection of a hash-function Hash. ISO/IEC 10118 specifies hash-functions. There shall be a binding between the signature mechanism and the hash-function in use. Without such a binding, an adversary might claim the use of a weak hash-function (and not the actual one) and thereby forge a signature.

The user of a digital signature mechanism should conduct a risk assessment considering the costs and benefits of the various alternative means of accomplishing the required binding. This assessment should include an assessment of the cost associated with the possibility of a bogus signature being produced.

NOTE 1 One of the security requirements for the hash-function Hash used in this part of ISO/IEC 9796 is so-called "collision-resistance."

NOTE 2 There are various ways to accomplish this binding. The following options are listed in order of increasing risk:

a) Require a particular hash-function when using a particular signature mechanism. The verification process shall exclusively use that particular hash-function. ISO/IEC 14888-3 gives an example of this option where the DSA mechanism requires the use of Dedicated Hash-function 3 (otherwise known as SHA-1) from ISO/IEC 10118-3;

b) Allow a set of hash-functions and explicitly indicate the hash-function in use in the certificate domain parameters. Inside the certificate domain, the verification process shall exclusively use the hash-function indicated in the certificate. Outside the certificate domain, there is a risk arising from certification authorities (CAs) that may not adhere to the user's policy. If, for example, an external CA creates a certificate permitting other hash-functions, then signature forgery problems may arise. In such a case a misled verifier may be in dispute with the CA that produced the other certificate; and

c) Allow a set of hash-functions and indicate the hash-function in use by some other method, e.g., an indication in the message or a bilateral agreement. The verification process shall exclusively use the hash-function indicated by the other method. However, there is a risk that an adversary may forge a signature using another hash-function.

NOTE 3 The "other method" referred to in paragraph c) immediately above could be in the form of a hash-function identifier included in the octet string representative d. If the hash-function identifier is included in d in this way then an attacker cannot fraudulently reuse an existing signature with the same octet string d_1 and a different d_2, even when the verifier could be persuaded to accept signatures created using a hash-function sufficiently weak that pre-images can be found. However, in this latter case and using the weak hash-function, an attacker can still find a new signature with a "random" d_1.

NOTE 4 The attack mentioned in Note 3 that yields a new signature with a "random" d_1 can be prevented by requiring the presence of a specific structure in d_1. For instance, one may impose a length limit on d_1 that is sufficiently less than the capacity of the signature scheme. For some digital signature schemes, a length limit on d_1 may also prevent an attacker from reusing existing signatures even if no hash-function identifier is included in the message representative, provided that the mask generation function MGF is based on the hash-function. This holds under the reasonable assumption that the weak hash-function involved is a "general purpose" hash-function, not one designed solely for the purpose of forging a signature.

6 Framework for digital signatures giving message recovery

6.1 Processes

Clauses 6.2 through 6.4 contain a high-level description of a general model for the six signature schemes specified in this part of ISO/IEC 9796. A detailed description of the general model is provided in Clause 7.

A digital signature scheme specified in this part of ISO/IEC 9796 is defined by the specification of the following processes:

— parameter generation process;

— signature generation process;

— signature verification process.

© ISO/IEC 2006 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

6.2 Parameter generation process

6.2.1 Domain parameters

The parameters can be divided into domain parameters and user keys. The domain parameters consist of parameters to define a finite group, such as a multiplicative group of a finite field or an additive group on an elliptic curve over a finite field, and other public information which is common to and known by or accessible to all entities within the domain. As well as the domain parameters specific to the cryptographic scheme in use, the following parameters must be specified:

— an identifier for the digital signature scheme used;

— the type of redundancy;

— (optional) a hash function Hash;

— the user key generation procedures.

For the implementation techniques and the mathematical background for an additive group on an elliptic curve over a finite field, ISO/IEC 15946-1 shall be referred. For the methods to construct an elliptic curve over a finite field, ISO/IEC 15946-5 shall be referred.

6.2.2 User keys

Each entity has its own public and private keys. The user keys of entity A consist of the following:

— the private signature key x_A;

— the public verification key Y_A;

— (optional) other information, which is specific to the entity A, for the use in the signature generation and/or verification process.

NOTE 1 User keys are valid only within the context of a specified set of domain parameters.

NOTE 2 The signature verifier may require assurance that the domain parameters and public verification key are valid, otherwise there is no assurance of meeting the intended security even if the signature verifies. The signer may also require assurance that the domain parameters and public verification key are valid, otherwise an adversary may be able to generate signatures that verify.

6.3 Signature generation process

The following data items are required for the signature generation process:

— the domain parameters;

— the signer A's private signature key x_A;

— a message M.

For all the schemes specified in this part of ISO/IEC 9796, the signature generation process consists of the following procedures:

a) splitting the message;

b) (optional) computation of redundancy, or computation of the message digest;

© ISO/IEC 2006 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

c) computations in a finite group, which is either the multiplicative group of a finite field or the additive group on an elliptic curve over a finite field;

d) computations modulo the group order of the base element G;

e) formatting the signed message.

The output of the signature generation process is a pair (r, s) that constitutes A's digital signature of the message M.

6.4 Signature verification process

The following data items are required for the signature verification process:

— the domain parameters;

— the signer A's public verification key Y_A;

— the non-recoverable part of the message M'_{clr} (if any);

— the received signature for M, represented as an octet string r' and an integer s'.

For all the schemes the signature verification process consists of some or all of the following procedures:

a) signature size verification;

b) computations in a finite group, which is either the multiplicative group of a finite field or the additive group on an elliptic curve over a finite field;

c) computations modulo the group order of the base element G;

d) recovering the data input or the message;

e) signature checking.

If all procedures are passed successfully, the signature is accepted by the verifier; otherwise it is rejected.

7 General model for digital signatures giving message recovery

7.1 Requirements

7.1.1 Domain parameters

Users who wish to employ one of the digital signature mechanisms specified in this part of ISO/IEC 9796 shall select the following domain parameters of the digital signature scheme:

a) an explicitly given finite field F, or an elliptic curve E over an explicitly given finite field F;

b) an element G in F or E of prime order n.

Agreement on these choices amongst the users is essential for the purpose of the operation of the digital signature mechanism giving message recovery.

NOTE 1 The size of n affects the level of security offered by the scheme and shall be chosen to meet the defined security objectives.

© ISO/IEC 2006 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

NOTE 2 The two possible groups with which this scheme may be used are normally written using multiplicative notation (for the multiplicative group of the finite field) and additive notation (for the group of points on an elliptic curve). In Clause 7, the multiplicative notation is used, in order to simplify the presentation.

NOTE 3 For the definition of an explicitly given finite field, see Clause A.3.

NOTE 4 For the definition of an elliptic curve over an explicitly given finite field, see Clause A.4.

NOTE 5 For efficient implementations and cryptographic techniques related to the groups on elliptic curves, see ISO/IEC 15946-1.

7.1.2 Type of redundancy

Users shall select the type of redundancy, which shall be

— natural redundancy,

— added redundancy, or

— both.

Agreement on the type of redundancy amongst the users is essential for the purpose of the operation of the digital signature mechanism giving message recovery.

If users use added redundancy, the length in octets of added redundancy, L_{red}, shall be fixed. A message with added redundancy may be constructed by the hash token of the message or of the recoverable message.

If users use natural redundancy alone, then L_{red} is set equal to 0. A message with natural redundancy means that the message includes redundancy naturally, such as the use of ASCII characters, or that the redundancy of the message is verifiable implicitly in some applications.

The natural or added redundancy may be anything agreed upon as long as it can be checked by the communicating parties. Total redundancy, which consists of natural redundancy and added redundancy, shall be greater than some minimum value specified by the application. In general natural redundancy alone shall only be used for total message recovery.

NOTE The value of the parameter L_{red} also affects the security level of the signatures giving message recovery.

7.2 Summary of functions and procedures

The signature schemes specified in this part of ISO/IEC 9796 give message recovery. More precisely, some of the data which is input to the signature generation function is recovered from the signature as part of the signature verification procedure.

The signature scheme consists of the following functions and procedures:

— user key generation process;

— signature generation process;

— signature verification process.

© ISO/IEC 2006 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

7.3 User key generation process

One of the following two methods shall be used to compute the key pair consisting of the public verification and the private signature key (the signing entity shall keep the private signature key secret):

a) Key generation I

Given a valid set of domain parameters, a private signature key and corresponding public verification key may be generated as follows:

1) Select a random or pseudorandom integer x_A in the set $[1, n-1]$. The integer x_A must be protected from unauthorised disclosure and be unpredictable;

2) Compute the element $Y_A = G^{x_A}$;

3) The key pair is (Y_A, x_A), where Y_A will be used as public verification key, and x_A is the private signature key.

To allow an unified representation of the algorithms, put $P = G$ and $Q = Y_A$.

b) Key generation II

Given a valid set of domain parameters, a private signature key and corresponding public verification key may be generated as follows:

1) Select a random or pseudorandom integer e in the set $[1, n-1]$ and compute an integer x_A in the interval $[1, n-1]$ with the property $x_A e = 1 \bmod n$. The integer x_A must be protected from unauthorised disclosure and be unpredictable;

2) Compute the element $Y_A = G^e$, and then erase the integer e in a secure manner;

3) The key pair is (Y_A, x_A), where Y_A will be used as public verification key, and x_A is the private signature key.

To allow an unified representation of the algorithms, put $P = Y_A$ and $Q = G$.

Prior to use of the public verification key the verifier shall have assurance about its validity and ownership. This validation may be obtained by various means, see Clause 6.2.2.

NOTE 1 Some schemes use the range $[1, n-2]$ for the private signature key x_A.

NOTE 2 Key generation I is the more popular method and is often used. In some environments where modular inversion is expensive, Key generation II might be useful.

7.4 Signature generation process

7.4.1 Procedures

Figure 1 shows the signature generation process, which consists of the following procedures:

a) producing a randomizer and the pre-signature;

b) splitting the message;

c) producing the data input;

d) computing the signature;

e) formatting the signed message.

NOTE Each mechanism may require scheme-dependent domain parameters other than those shown in Figure 1.

© ISO/IEC 2006 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

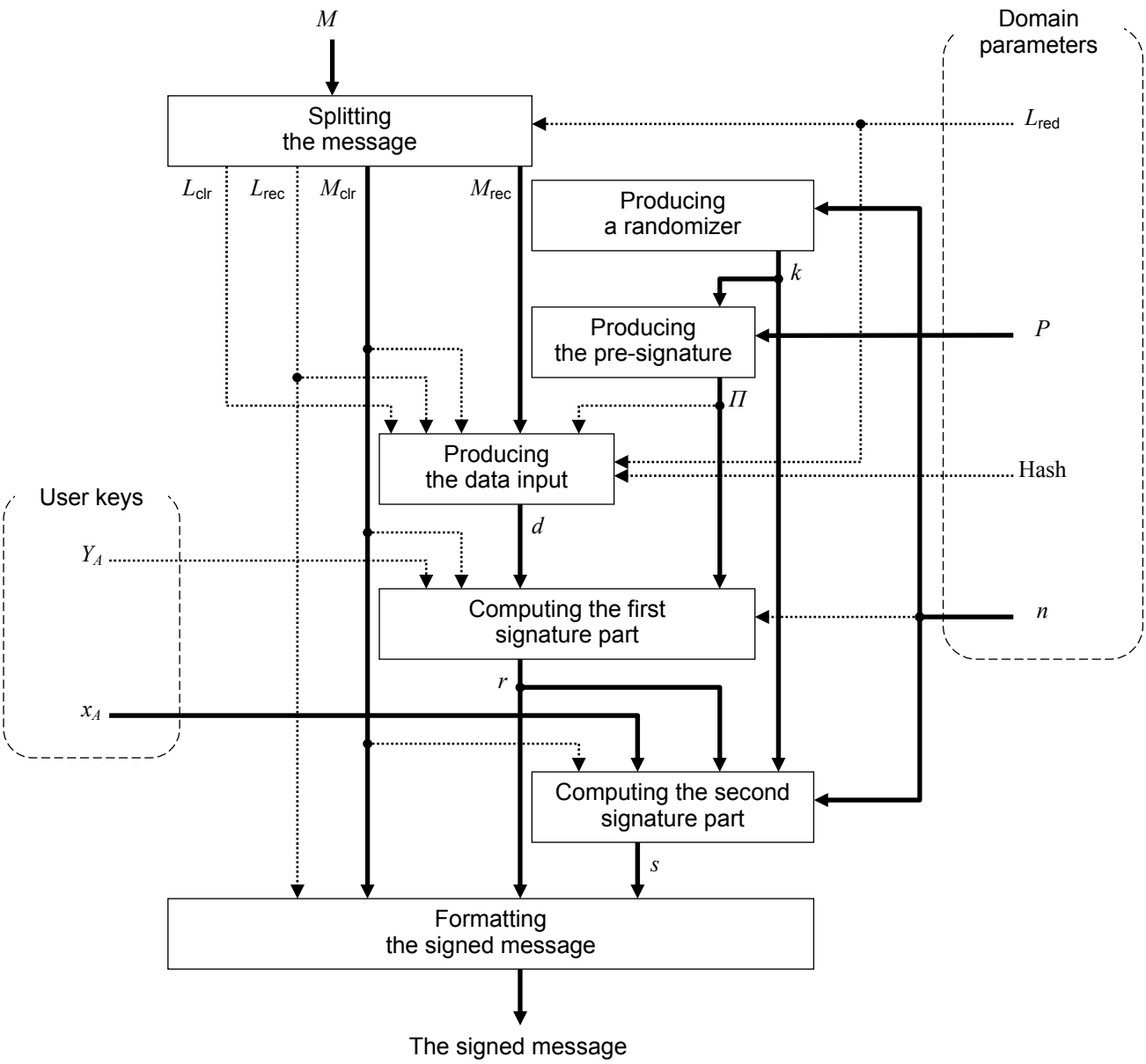

Figure 1 — The signature generation process

© ISO/IEC 2006 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

7.4.2 Producing a randomizer and the pre-signature

Prior to each signature computation the signing entity must have a fresh, secret randomizer value available. The randomizer is an integer k such that $1 \le k \le n-1$. The implementation of the signature scheme must ensure that the following two requirements are satisfied:

— randomizer generation shall be executed in such a way that the probability that the same randomizer is used to produce signatures for two different messages shall be negligible;

— used randomizer values shall never be disclosed; once used, they shall be destroyed.

First a randomizer k, which is an integer, is produced. Then the pre-signature Π, which is an octet string, is computed as a function of the randomizer. The pre-signature is an intermediate data item that is produced during the signature generation process in any randomized signature mechanism. The pre-signature is a public data item, while the value of the randomizer shall be available only to the signature generation process.

NOTE 1 Disclosure of a randomizer after use may jeopardise the secrecy of the private key. Used randomizers are never required again by the signer or verifier and should be securely erased. If the same value of the randomizer is used to produce signatures for two different messages, or if the randomizer for a signature is disclosed, then it might be possible to recover the private key from the signatures.

NOTE 2 Randomizers may be produced and corresponding pre-signatures may be computed offline. In this case, the randomizers should be stored securely for future use by the signature generation process.

7.4.3 Splitting the message

The message M is split into the recoverable part M_{rec} and the non-recoverable part M_{clr} of the message, and L_{rec} and L_{clr} are defined to be the length in octets of the recoverable part M_{rec} and the non-recoverable part M_{clr}, respectively.

7.4.4 Producing the data input

The input to the data input function is the recoverable part of the message M_{rec} with added redundancy, or the recoverable part of the message M_{rec} with natural redundancy. The inputs may optionally include the non-recoverable part M_{clr} , the lengths L_{rec} and L_{clr}. If added redundancy is used, the data input involves producing the hash-token. The hash-token is formed by the hash-code itself, or with the hash-function identifier concatenated to the right of the hash-code, where the hash-code is computed by hashing the (recoverable part of) message. The choice of whether or not the hash-token includes the hash-function identifier shall be controlled by the domain parameters. The output of the data input function is d, which is an octet string.

NOTE 1 The choice of data input may be determined by each application or signature scheme.

NOTE 2 See Annex D for an example method of producing the data input with added redundancy.

7.4.5 Computing the signature

The signatures produced by the schemes in this part of ISO/IEC 9796 have two parts r and s. The first part r is an octet string which is computed as a function of the pre-signature Π and the data input d (and optionally other parameters), where d is an octet string that depends upon the message. The second part s is an integer such that $0 < s < n$ and computed as a function of the first part r, the randomizer k, and the private signature key x_A (and optionally other parameters).

© ISO/IEC 2006 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

7.4.6 Formatting the signed message

Knowledge of the length of the recoverable part of the message is necessary for the successful opening and verification of the signed message. This information must be given by the domain parameter, included in the signed message and/or retrieved from the data input d.

The signed message consists of the following data items:

— the non-recoverable part M_{clr} of the message;

— the first part r of the signature;

— the second part s of the signature;

— (optional) the length L_{rec} of the recoverable part of the message.

7.5 Signature verification process

7.5.1 Procedures

Figure 2 shows the signature verification process, which consists of the following procedures:

a) opening the signed message;

b) signature size verification;

c) recovering the pre-signature or the data input;

d) recovering the data input or the message;

e) re-computing the hash-token(optional);

f) checking the signature.

© ISO/IEC 2006 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

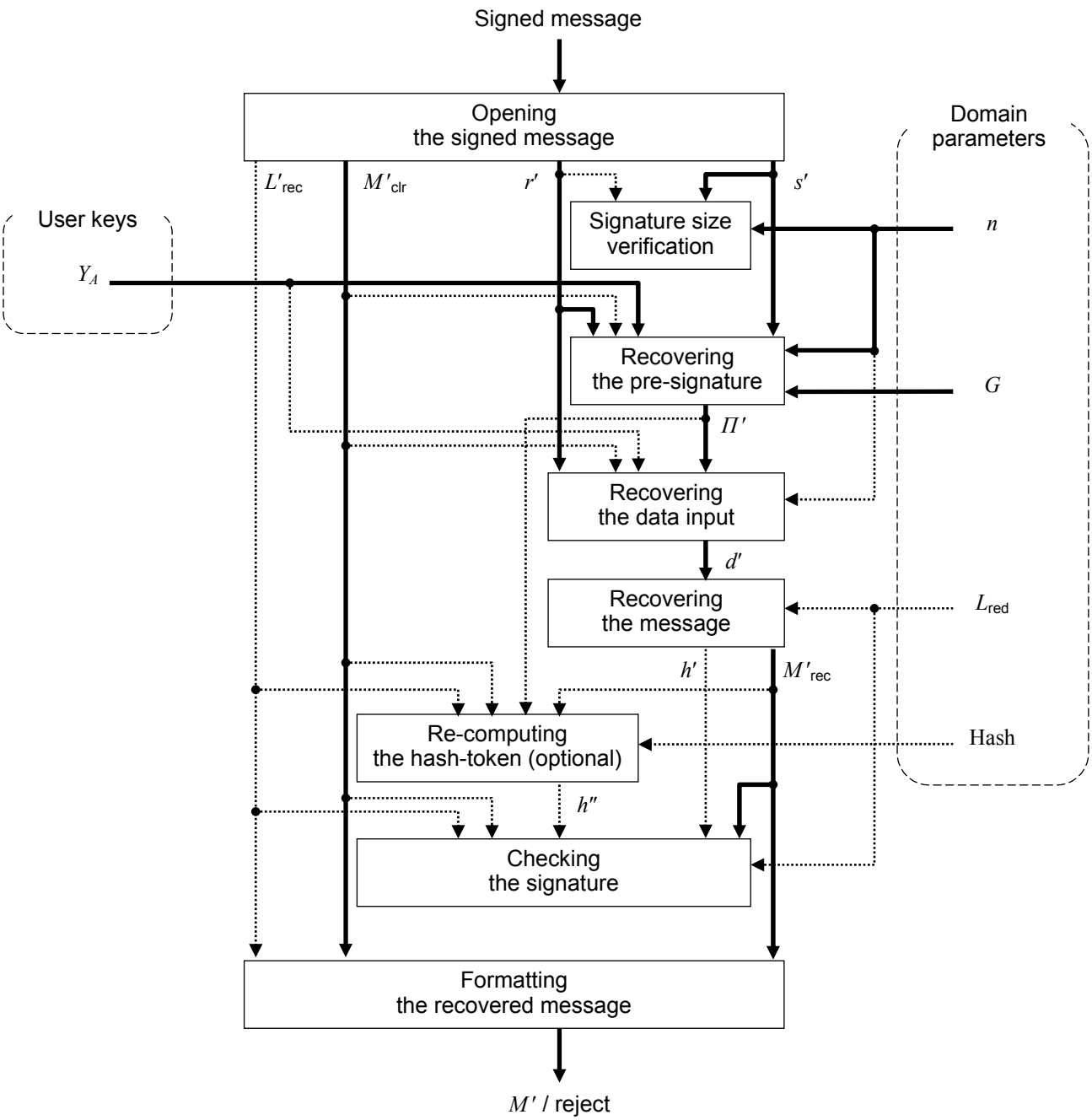

Figure 2 — Signature verification process

Checking the signature consists of

— comparing the recovered and recomputed (truncated) hash-tokens, or

— verifying the redundancy.

© ISO/IEC 2006 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)

7.5.2 Opening the signed message

When starting this step, the verifier must have the following information available:

— the lengths of the different signature/message parts included in the signed message;

— the value of the parameter L_{red}.

The verifier extracts the following different parts of the signed message:

— the non-recoverable part of the message;

— the first part r' of the signature;

— the second part s' of the signature;

— (optional) the length L'_{rec} of the recoverable message part.

7.5.3 Signature size verification

The verifier shall verify the size of the parts of a signature.

7.5.4 Recovering the pre-signature

At the beginning of this step the verifier must have the following information available:

— the public parameters which specify the signature scheme in use;

— the public verification key Y_A of the signing entity.

The computations in this step are specific to the signature scheme in use. The pre-signature is determined by the public verification key Y_A. Given the signature (r', s'), the pre-signature Π' is recovered.

7.5.5 Recovering the data input or the message

Given the first part r' of the signature and the recovered pre-signature Π', the data input d' is recovered. The recovered data input d' is an octet string.

7.5.6 Re-computing the hash-token (optional)

First, the hash-function used by the signing entity in Clause 7.4 is identified, possibly by the domain parameter and/or by retrieving the hash-function identifier from the recovered hash-token. Then the hash-code is recomputed by hashing the message.

The recomputed hash-code is used to obtain the recomputed hash-token by optionally concatenating the hash-function identifier.

7.5.7 Checking the signature

Checking the signature consists of

— comparing the recomputed (truncated) hash-token h'' with the recovered (truncated) hash-token h', or

— verifying the added, and/or natural redundancy of the recovered message.

© ISO/IEC 2006 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO IEC 09796-3-2006 (2013)