INTERNATIONAL STANDARD

ISO/IEC 14888-2

Second edition
2008-04-15

Information technology — Security techniques — Digital signatures with appendix

Part 2: Integer factorization based mechanisms

Technologies de l'information — Techniques de sécurité — Signatures numériques avec appendice

Partie 2: Mécanismes basés sur une factorisation entière

Reference number
ISO/IEC 14888-2:2008(E)

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

Page

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 14888-2 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 14888-2:1999), which has been technically revised.

ISO/IEC 14888 consists of the following parts, under the general title *Information technology — Security techniques — Digital signatures with appendix*:

— *Part 1: General*

— *Part 2: Integer factorization based mechanisms*

— *Part 3: Discrete logarithm based mechanisms*

Introduction

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

NOTE There are two series of International Standards specifying digital signatures. In both series, Part 2 specifies integer factorization based mechanisms and Part 3 specifies discrete logarithm based mechanisms.

- ISO/IEC 9796 [28] specifies signatures giving message recovery. As all or part of the message is recovered from the signature, the recoverable part of the message is not empty. The signed message consists of either the signature only (when the non-recoverable part of the message is empty), or both the signature and the non-recoverable part.
- ISO/IEC 14888 specifies signatures with appendix. As no part of the message is recovered from the signature, the recoverable part of the message is empty. The signed message consists of the signature and the whole message.

Most digital signature schemes involve three basic operations.

- An operation that produces key pairs. Each pair consists of a private signature key and a public verification key.
- An operation that makes use of a private signature key to produce signatures.
  - When, for a given message and private signature key, the probability of obtaining the same signature twice is negligible, the operation is probabilistic.
  - When, for a given message and private signature key, all the signatures are identical, the operation is deterministic.
- A deterministic operation that makes use of a public verification key to verify signed messages.

For each scheme, given the public verification key (but not the private signature key) and any set of signed messages (each message having been chosen by the attacker), the attacker should have a negligible probability of producing:

- a new signature for a previously signed message;
- a signature for a new message;
- the private signature key.

The title of ISO/IEC 14888-2 has changed, from *Identity-based mechanisms* (first edition) to *Integer factorization based mechanisms* (second edition).

a) The second edition includes the identity-based scheme specified in ISO/IEC 14888-2:1999, namely the GQ1 scheme. This scheme has been revised due to the withdrawal of ISO/IEC 9796:1991 in 1999.

b) Among the certificate-based schemes specified in ISO/IEC 14888-3:1998, it includes all the schemes based on the difficulty of factoring the modulus in use, namely, the RSA, RW and ESIGN schemes. These schemes have been revised due to the withdrawal of ISO/IEC 9796:1991 in 1999.

c) It takes into account ISO/IEC 14888-3:1998/Cor.1:2001, technical corrigendum to the ESIGN scheme.

d) It includes a format mechanism, namely the PSS mechanism, already specified in ISO/IEC 9796-2:2002, and details of how to use it in each of the RSA, RW, GQ1 and ESIGN schemes.

NOTE Similar format mechanisms have proofs of security [2], even without a salt.

e) It includes new certificate-based schemes that use no format mechanism, namely, the GQ2, GPS1 and GPS2 schemes.

f) For each scheme and its options, as needed, it provides an object identifier.

ISO and IEC draw attention to the fact that it is claimed that compliance with this document may involve the use of patents.

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

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

Patent holder	Patent number(s)	Subject
NTT 20-2 Nishi-shinjuku 3-Chome Shinjuku-ku Tokyo 163-1419, Japan	US 4 625 076	ESIGN (see Clause 11)
France Telecom R&D [a] Service PIV 38-40 Rue du Général Leclerc F 92794 Issy les Moulineaux Cedex 9, France	US 5 140 634, EP 0 311 470 EP 0 666 664	GQ1 (see Clause 7) GPS1 (see Clause 9)
Philips International B.V. Corporate Patents and Trademarks P.O. Box 220 5600 AE Eindhoven, The Netherlands	US 5 140 634, EP 0 311 470	GQ1 (see Clause 7)
University of California Senior Licensing Officer Office of Technology Transfer 1111 Franklin Street, 5th floor Oakland, California 94607-5200, USA	US 6 266 771	PSS (see 6.4 when using salt and 11.4)

[a] France Telecom claims that patent applications are pending in relation to GQ2 (see Clause 8) and GPS2 (see Clause 10). The patent numbers will be provided when available. ISO/IEC will then request the appropriate statements.

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.

Information technology — Security techniques — Digital signatures with appendix

Part 2: Integer factorization based mechanisms

1 Scope

This part of ISO/IEC 14888 specifies digital signatures with appendix whose security is based on the difficulty of factoring the modulus in use. For each signature scheme, it specifies:

a) the relationships and constraints between all the data elements required for signing and verifying;

b) a signature mechanism, i.e., how to produce a signature of a message with the data elements required for signing;

c) a verification mechanism, i.e., how to verify a signature of a message with the data elements required for verifying.

The production of key pairs requires random bits and prime numbers. The production of signatures often requires random bits. Techniques for producing random bits and prime numbers are outside the scope of this part of ISO/IEC 14888. For further information, see ISO/IEC 18031 [33] and ISO/IEC 18032 [34].

Various means are available to obtain a reliable copy of the public verification key, e.g., a public key certificate. Techniques for managing keys and certificates are outside the scope of this part of ISO/IEC 14888. For further information, see ISO/IEC 9594-8 [27], ISO/IEC 11770 [31] and ISO/IEC 15945 [32].

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 14888-1, *Information technology — Security techniques — Digital signatures with appendix — Part 1: General*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 14888-1 and the following apply.

3.1
modulus
integer whose factorization shall be kept secret and whose factors shall be infeasible to compute

3.2
representative
bit string produced by a format mechanism

3.3
salt
optional bit string for producing a representative

3.4
signature exponent
secret exponent for producing signatures

3.5
trailer
optional bit string on the right of a representative

3.6
verification exponent
public exponent for verifying signed messages and sometimes also for producing signatures

4 Symbols and abbreviated terms

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

$A \| B$ bit string resulting from concatenating the two bit strings A and B in that order

$A \oplus B$ bit string resulting from exclusive-oring the two bit strings A and B, of the same length

b adaptation parameter (GQ2)

Cr CRT coefficient

CRT Chinese Remainder Theorem

$|D|$ bit length of D if D is a bit string, or bit size of D if D is a number (i.e., 0 if $D = 0$, or the unique integer i so that $2^{i-1} \le D < 2^i$ if $D > 0$, e.g., $|65\,537 = 2^{16}+1| = 17$)

$\lfloor D \rfloor$ the greatest integer less than or equal to D

$\lceil D \rceil$ the least integer greater than or equal to D

E salt (RSA, RW, ESIGN)

F representative (RSA, RW, GQ1, ESIGN)

f number of prime factors

G, G_i public number

g, g_i base number

$(g \mid n)$ Jacobi symbol of a positive integer g with respect to an odd composite integer n

NOTE 1 By definition, the Jacobi symbol of g with respect to n is the product of the Legendre symbols of g with respect to each prime factor of n (repeating the Legendre symbols for repeated prime factors). The Jacobi symbol [13, 15] can be efficiently computed without knowledge of the prime factors of n.

$(g \mid p)$	Legendre symbol of a positive integer g with respect to an odd prime integer p

NOTE 2 By definition, if p is prime, then $(g \mid p) = g^{(p-1)/2} \bmod p$. This means that $(g \mid p)$ is zero if g is a multiple of p, and either $+1$ or -1 otherwise, depending on whether or not g is a square modulo p.

$\gcd(a, b)$	the greatest common divisor of the two positive integers a and b
H, HH	hash-codes
h	hash-function
$i \bmod n$	the unique integer j from 0 to $n-1$ such that n divides $i - j$
Id	sequence of identification data (GQ1)
$Indic$	indicator of a mechanism in use (hash-function, format mechanism, hash-variant)
k	security parameter (GQ2)
$\mathrm{lcm}(a, b)$	the least common multiple of the two positive integers a and b
M	message
m	number of base numbers (GQ2)
n	modulus
p_i	prime factor
Q, Q_i	private number
$Q_{i,j}$	private component (GQ2)
R	first part of signature (GQ1, GQ2, GPS1, GPS2)
r, r_i, $r_{i,j}$	random number (GQ1, GQ2, GPS1, GPS2, ESIGN)
S	signature (RSA, RW, ESIGN) or second part of signature (GQ1, GQ2, GPS1, GPS2)
s, s_i	signature exponent (RSA, RW, GQ1, GQ2)
T	coupon (GPS1, GPS2)
t	signature length parameter (GQ1, GQ2)
u, u_i	exponent (GQ1, GQ2)
v	verification exponent (RSA, RW, GQ1, GPS2, ESIGN)
W	bit string (GQ1, GQ2, GPS1, GPS2)
$'XY'$	notation using the hexadecimal digits '0' to '9' and 'A' to 'F', equal to XY to the base 16
x, y, z	integers
α	bit size of the moduli
γ	bit length of the representatives (RSA, RW, GQ1, ESIGN)
ε	bit length of the salts (format mechanisms)
τ	bit length of the trailers (format mechanisms)

5 General

5.1 Security requirements

The signature mechanism makes use of a set of data elements required for signing. This set includes the signer's private signature key, which is referred to simply as the “signature key” in this document. Some data elements of the signature key shall be kept secret (there is at least one secret data element).

NOTE Every secret data element should remain confined within a piece of hardware or software under the control of the signer, in such a way that it is infeasible for an attacker to extract it. Integrated circuit cards [24] may produce signatures. Protection profiles for signature production devices are outside the scope of this document.

The production of RSA and RW signatures is probabilistic when and only when every signature requires a fresh salt. The production of GQ1, GQ2, GPS1, GPS2 and ESIGN signatures is essentially probabilistic. When the production of signatures is probabilistic, every signer shall have the means to select random bits.

The verification mechanism makes use of a set of data elements required for verifying, all of which shall be made public within the domain.

- Every public data element common to all signers is known as a domain parameter.
- Every public data element specific to a single signer shall be part of the signer's public verification key, which is referred to simply as the “verification key” in this document.

Within a given domain, every verifier shall know the set of domain parameters and shall obtain a reliable copy of the signer's verification key.

The signer and the verifier shall have adequate assurance that the set of domain parameters is valid, i.e., that it satisfies the constraints specific to the scheme. Otherwise, there is no assurance of meeting the intended security even if the signed message is accepted. This assurance may be obtained in various ways, including one or more of:

a) selection of a set of values from a trusted published source, e.g., an International Standard;

b) production of a set of values by a trusted third party, e.g., a certification authority [27];

c) validation of a set of values by a trusted third party, e.g., a certification authority [27];

d) for the signer, production of a set of values by a trusted system;

e) for the signer and the verifier, validation of a set of values.

The signer and the verifier shall have adequate assurance that the verification key is valid, i.e., that it satisfies the constraints specific to the scheme. This assurance may be obtained in various ways, including one or more of:

a) access to a directory or verification of a certificate;

b) a key validation protocol operating on the verification key and possibly other information, perhaps involving an interaction with the piece of hardware or software producing signatures;

c) trust in another party's assertion of having obtained assurance that the verification key is valid;

d) trust that the key production has been implemented correctly.

Specific key validation protocols and methods for obtaining and conveying assurance of key validity are outside the scope of this document.

The security of every signature scheme specified in this document relies upon a modulus and a hash-function.

- A modulus is secure (i.e., factorization-resistant) as long as no factor has been revealed. In the context of use of the scheme, no entity shall be able to effectively factor the modulus in use.
- The hash-function in use shall be one of those specified in ISO/IEC 10118; it should be collision-resistant.

5.2 Verification keys

Table 1 summarizes the verification keys (see 6.1, 7.1, 8.1, 9.1, 10.1 and 11.1).

Table 1 — Verification keys

Scheme	Mandatory	Optional [a]		Optional [b]	
RSA, RW, ESIGN	n	v	*Indic*(h)	α	*Indic*(format, ε, τ)
GQ1 [c]		n, v	*Indic*(h)	α	*Indic*(variant), *Indic*(format, ε, τ)
GQ2	n		*Indic*(h)	b, (g_1, g_2 … g_m), α	*Indic*(variant)
GPS1	G	n	*Indic*(h)	g, α	*Indic*(variant)
GPS2	n	v	*Indic*(h)	g, α	*Indic*(variant)

[a] If not part of the verification key, such a data element shall be a domain parameter.
[b] If neither a domain parameter, nor part of the verification key, such a data element shall take a default value.
[c] The GQ1 verification key may be empty.

Every signature scheme specified in this document makes use of a modulus, denoted n.

- In the RSA, RW, GQ2, GPS2 and ESIGN schemes, the verification key shall include n.
- In the GQ1 and GPS1 schemes, either the domain parameters or the verification key shall include n.

NOTE The use of a given modulus is normally limited to a given period of time within a given domain.

To prescribe the bit size of the modulus in use, either the domain parameters or the verification key may include a data element, denoted α. If α is not included, then the default value of α is set equal to the bit size of the modulus in use (i.e., the modulus size is not prescribed).

In the GPS1 scheme, the verification key shall include the public number in use, denoted G.

For compatibility with public key infrastructures already deployed, even when all the signers use the same value within the domain, the verification key may include:

— the verification exponent in use, denoted v, in the RSA, RW, GQ1, GPS2 and ESIGN schemes;

— the modulus in use, denoted n, in the GQ1 and GPS1 schemes.

Every signature scheme specified in this document makes use of a hash-function, denoted h.

- In the RSA, RW and ESIGN schemes, a format mechanism makes use of h to convert messages into representatives, and to check recovered representatives.
- In the GQ1 scheme, a format mechanism makes use of h to convert sequences of identification data into public numbers, and a hash-variant makes use of h to produce bit strings.
- In the GQ2, GPS1 and GPS2 schemes, a hash-variant makes use of h to produce bit strings.

To indicate the hash-function in use, either the domain parameters or the verification key shall include a data element, denoted *Indic*(h).

This document specifies three format mechanisms (PSS in 6.4, 7.4 and 11.4; D1 and D2 in Annex D). Each format mechanism makes use of two parameters, denoted ε and τ. Set to 0, 64 or $|H|$, ε indicates the bit length of the salts. Set to 0, 8 or 16, τ indicates the bit length of the trailers.

This document specifies four hash-variants, where W denotes a bit string and M a message.

1) h(W || M) 2) h(W || h(M)) 3) h(h(W) || M) 4) h(h(W) || h(M))

To indicate the format mechanism in use, together with the options ε and τ in use, and/or the hash-variant in use, either the domain parameters or the verification key may include one or two data elements, denoted *Indic*(format, ε, τ) and *Indic*(variant), as needed.

Key precedence — When the domain parameters and the verification key include the same data element with different values, the verification key shall take precedence.

NOTE Within a given domain, owing to key precedence, different signers may make use of different hash-functions and/or different modulus sizes.

5.3 CRT technique

Consider two integers x_1 and x_2 that are co-prime, but not necessarily prime. By definition, the CRT coefficient of x_1 and x_2, denoted Cr, is the unique positive integer, less than x_1, such that $Cr \times x_2 - 1$ is a multiple of x_1.

Any integer X from $\{0, 1 \ldots x_1 \times x_2 - 1\}$ may be decomposed into the unique pair of components $X_1 = X \bmod x_1$ from $\{0, 1 \ldots x_1 - 1\}$ and $X_2 = X \bmod x_2$ from $\{0, 1 \ldots x_2 - 1\}$.

The CRT composition reverses the above decomposition. It makes use of the three integers x_1, x_2 and Cr to convert any two components X_1 from $\{0, 1 \ldots x_1 - 1\}$ and X_2 from $\{0, 1 \ldots x_2 - 1\}$, into the unique integer X from $\{0, 1 \ldots x_1 \times x_2 - 1\}$ such that $X_1 = X \bmod x_1$ and $X_2 = X \bmod x_2$.

$$Y = X_1 - X_2 \mod x_1;\ Z = Y \times Cr \mod x_1;\ X = Z \times x_2 + X_2$$

In order to convert three components X_1 from $\{0, 1 \ldots x_1 - 1\}$, X_2 from $\{0, 1 \ldots x_2 - 1\}$ and X_3 from $\{0, 1 \ldots x_3 - 1\}$, where x_1, x_2 and x_3 are pairwise co-prime, into the unique integer X from $\{0, 1 \ldots x_1 \times x_2 \times x_3 - 1\}$ so that $X_1 = X \bmod x_1$, $X_2 = X \bmod x_2$ and $X_3 = X \bmod x_3$, the CRT composition is used twice:

1) to compute T from $\{0, 1 \ldots x_1 \times x_2 - 1\}$ so that $X_1 = T \bmod x_1$ and $X_2 = T \bmod x_2$;
2) to compute X from $\{0, 1 \ldots x_1 \times x_2 \times x_3 - 1\}$ so that $T = X \bmod x_1 \times x_2$ and $X_3 = X \bmod x_3$.

When the prime factors of n are available (see 6.2, 7.1, 8.1, 8.2, 9.1, 9.2.2 and 10.2.2), the CRT technique reduces the complexity of arithmetic computations mod n (see B.2.3). Rather than directly computing a global result from $\{0, 1 \ldots n-1\}$, a set of components is computed and then converted into the global result.

NOTE The CRT technique efficiency increases in terms of the number of distinct prime factors.

5.4 Conversions between bit strings, integers and octet strings

A bit string, denoted D, consists of $|D|$ bits, where the value of each bit is 0 or 1; the bits are numbered from the leftmost bit, denoted d_1, to the rightmost bit, denoted $d_{|D|}$.

$$D = d_1\ d_2\ d_3 \ldots d_{|D|-1}\ d_{|D|}$$

To convert D into an integer, denoted A, the leftmost bit, denoted d_1, is the most significant bit, and the rightmost bit, denoted $d_{|D|}$, is the least significant bit.

$$A = 2^{|D|-1} \times d_1 + 2^{|D|-2} \times d_2 \ldots + 2^2 \times d_{|D|-2} + 2 \times d_{|D|-1} + d_{|D|}$$

The bit size of integer A, denoted $|A|$ (i.e., $2^{|A|-1} \le A < 2^{|A|}$ if $A > 0$, noting that $0 \le A < 2^{|D|}$), is either equal to $|D|$ if $d_1 = 1$, or less than $|D|$ if $d_1 = 0$. The binary representation of integer A by a bit string of length greater than $|A|$ is the unique bit string which, when converted to an integer, gives A.

When the bit length of a string is a multiple of eight, the bit string is conveniently represented by an octet string where each octet has a value from '00' to 'FF' in the hexadecimal notation. In an octet string, the octets are numbered from the leftmost octet to the rightmost octet. To convert an octet string into an integer, the leftmost octet is the most significant octet and the rightmost octet is the least significant octet.

6 RSA and RW schemes [1]

6.1 Data elements required for signing/verifying

The subsequent relationships and constraints apply to the following data elements:

- a verification exponent;
- a set of distinct prime factors;
- a modulus;
- a signature exponent;
- a set of CRT signature exponents.

The verification exponent is denoted v. The values $v = 0$ and $v = 1$ are forbidden.

NOTE The values v = 2, 3 and 65 537 ($= 2^{16}+1$) have some practical advantages.

The set of distinct prime factors is denoted $p_1, p_2 \ldots p_f$ in ascending order ($f > 1$).

The RSA scheme makes use of an odd verification exponent. There may be more than two prime factors ($f \geq 2$). For i from 1 to f, v shall be co-prime to $p_i - 1$, i.e., $\gcd(v, p_i - 1) = 1$.

The RW scheme makes use of an even verification exponent. This document mandates the value $v = 2$, with only two prime factors ($f = 2$), both congruent to 3 mod 4, but not congruent to each other mod 8.

The modulus, denoted n, is the product of the prime factors ($n = p_1 \times \ldots \times p_f$). Its size shall be α bits.

The signature exponent is denoted s. It is any positive integer (the least one is often used) so that $v \times s - 1$ is a multiple of either $\mathrm{lcm}(p_1 - 1, \ldots p_f - 1)$ if v is odd, or $\mathrm{lcm}(p_1 - 1, p_2 - 1)/2$ if $v = 2$.

The set of CRT signature exponents is denoted s_1 to s_f. For i from 1 to f, s_i is any positive integer (the least one is often used) so that $v \times s_i - 1$ is a multiple of either $p_i - 1$ if v is odd, or $(p_i - 1)/2$ if $v = 2$.

NOTE In the RW scheme, as a prime factor is congruent to $3 \bmod 8$ and the other one to $7 \bmod 8$, $n \equiv 5 \bmod 8$, $(\pm 2 \mid n) = -1$, $s = (n - p_1 - p_2 + 5)/8$, $s_1 = (p_1 + 1)/4$ and $s_2 = (p_2 + 1)/4$.

Signing requires a hash-function (see 5.1), a format mechanism and a signature key. The format mechanism specified in 6.4 is recommended; it makes use of two parameters, denoted ε and τ. The signature key takes either of two forms:

- With CRT: p_1 to p_f, $f - 1$ CRT coefficients (see 5.3) and s_1 to s_f.
- Without CRT: n and s (n public).

NOTE The format mechanism specified in 6.4 is believed to be secure. The two format mechanisms specified in Annex D have a smaller safety margin.

Verifying requires a set of domain parameters and a verification key. Either the domain parameters or the verification key shall include v and $Indic(\mathrm{h})$, and may include α (by default, $\alpha = |n|$) and $Indic(\text{format}, \varepsilon, \tau)$ (by default, 6.4 with the options $\varepsilon = |H|$ and $\tau = 8$). The verification key shall include n.

---

[1] The RSA scheme is due to Rivest, Shamir and Adleman [4, 19]. It makes use of a permutation of the ring of the integers modulo n.

The RW scheme is due to Rabin [18] and Williams [23]. It makes use of a permutation of a subset of the ring of the integers modulo n, namely, the set of the elements less than $n/2$ and having +1 as Jacobi symbol with respect to n.

6.2 Signature mechanism

Illustrated in Figure 1, the mechanism makes use of a hash-function, a format mechanism and a signature key, to sign a message (a bit string, denoted M), i.e., to produce a signature of M (a bit string, denoted S).

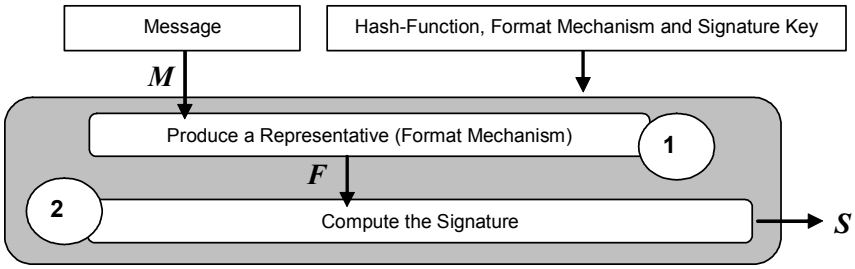

Figure 1 — Signing with RSA or RW

Stage 1 — Convert the message M into a representative of $\gamma = |n|$ bits, denoted F, in accordance with the format mechanism in use. The bit string F represents a number, divisible by four, also denoted F $(0 < F < n)$.

Stage 2 — Produce a number, denoted G $(0 < G < n)$.

- If v is odd, then $G = F$.
- If $v = 2$, evaluate the Jacobi symbol $(F \mid n)$ and force the Jacobi symbol $(G \mid n)$ to $+1$.
  - If $(F \mid n) = +1$, then $G = F$.
  - If $(F \mid n) = -1$, then $G = F / 2$.
  - If $(F \mid n) = 0$ (a very unlikely case), then the procedure fails.

Produce a number, denoted S, in either of two ways.

- With CRT, for i from 1 to f, compute $G_i = G \bmod p_i$ and $S_i = G_i^{s_i} \bmod p_i$. The number S is the CRT composition (see 5.3) of S_1 to S_f.
- Without CRT, compute $S = G^s \bmod n$.

If $v = 2$, then the number S may be replaced by $n - S$.

The signature is any bit string representing S, often a string of $|n|$ bits, and is also denoted S.

6.3 Verification mechanism

Illustrated in Figure 2, the mechanism makes use of a set of domain parameters and a verification key (see Table 1), with key precedence (see 5.2), to verify a message and a signature of that message, i.e., the two bit strings, denoted M and S.

Stage 0 — Reject if $|n| \neq \alpha$, or if $v = 0$ or 1, or if n is not congruent to $5 \bmod 8$ when $v = 2$.

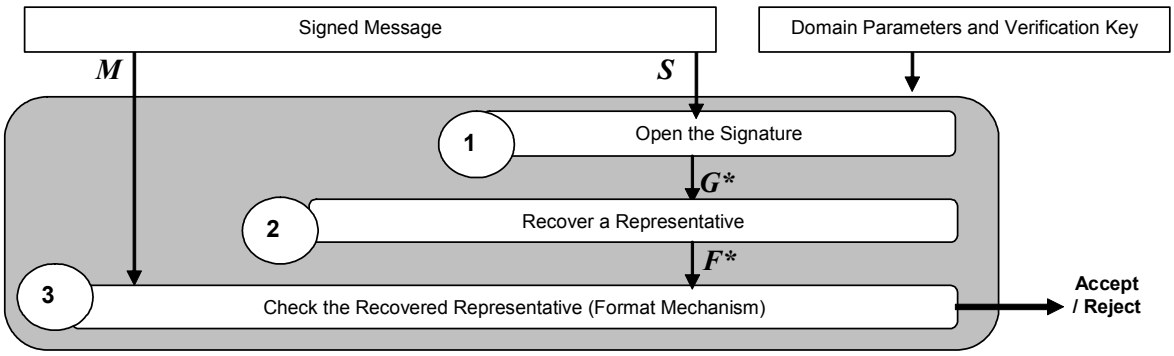

Figure 2 — Verifying with RSA or RW

Stage 1 — The bit string S represents a number, also denoted S. Reject if $S = 0$ or 1, or if $S \geq n-1$.

Compute $G^* = S^v \bmod n$.

Stage 2 — Recover a representative, denoted F^*.

- If v is odd, F^* is the string of $|n|$ bits representing G^*.
- If $v = 2$, F^* is the string of $|n|$ bits representing:
  - G^* if G^* is congruent to $4 \bmod 8$;
  - $n - G^*$ if G^* is congruent to $1 \bmod 8$;
  - $2\ G^*$ if G^* is congruent to $6 \bmod 8$;
  - $2\ (n - G^*)$ if G^* is congruent to $7 \bmod 8$.
  - Reject in any other case (the trailer cannot be interpreted).

Stage 3 — Check the recovered representative F^* in accordance with the format mechanism in use.

6.4 Format mechanism [2]

Convert the message M, making use of two parameters (ε indicates the length of the salt and τ indicates the length of the trailer), into a representative of γ bits, denoted F. Figure 3 illustrates the mechanism.

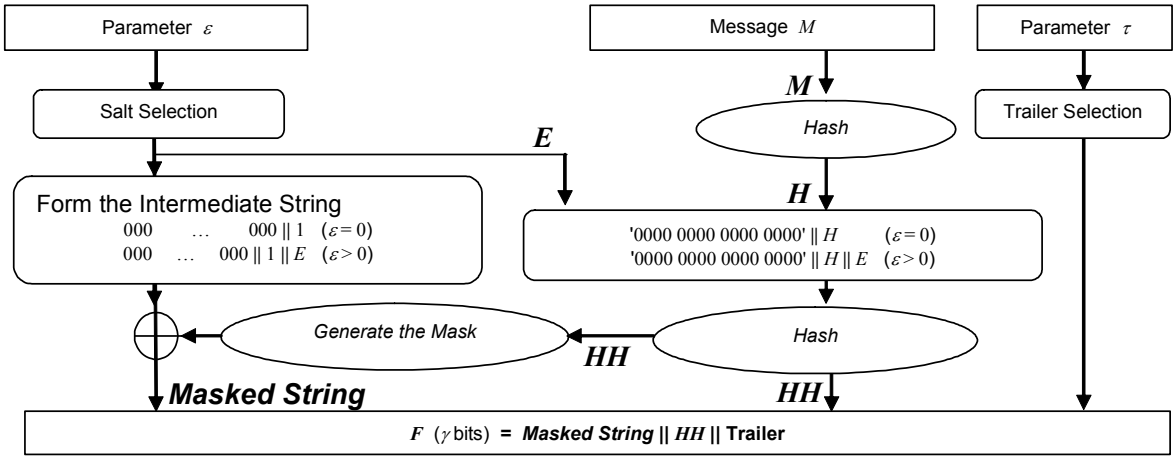

Figure 3 — Production of a representative

[2] This mechanism is due to Bellare and Rogaway [1]. When the salt has a fresh value for each signature, the resulting signature scheme is known as either RSA-PSS, or RW-PSS, where PSS stands for “Probabilistic Signature Scheme”.