INTERNATIONAL STANDARD

ISO/IEC 9798-5

Second edition
2004-12-01

Information technology — Security techniques — Entity authentication —

Part 5: Mechanisms using zero-knowledge techniques

Technologies de l'information — Techniques de sécurité — Authentification d'entité —

Partie 5: Mécanismes utilisant des techniques à divulgation nulle

Reference number
ISO/IEC 9798-5:2004(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 9798-5 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 9798-5:1999), which has been technically revised.

ISO/IEC 9798 consists of the following parts, under the general title *Information technology — Security techniques — Entity authentication*:

- *Part 1: General*
- *Part 2: Mechanisms using symmetric encipherment algorithms*
- *Part 3: Mechanisms using digital signature techniques*
- *Part 4: Mechanisms using a cryptographic check function*
- *Part 5: Mechanisms using zero-knowledge techniques*
- *Part 6: Mechanisms using manual data transfer*

Introduction

This document specifies authentication mechanisms in the form of exchanges of information between a claimant and a verifier.

In accordance with the types of calculations that need to be performed by the claimant and the verifier (see Annex C), the mechanisms can be classified into the following four main groups.

— The first group (Clauses 5 and 6) is characterized by the performance of short modular exponentiations. The challenge size needs to be optimized since it has a proportional impact on workloads.

— The second group (Clauses 7 and 8) is characterized by the possibility of a "coupon" strategy for the claimant. A verifier can authenticate a claimant with very limited computational power. The challenge size has no practical impact on workloads.

— The third group (Clause 9.3) is characterized by the possibility of a "coupon" strategy for the verifier. A verifier with very limited computational power can authenticate a claimant. The challenge size has no impact on workloads.

— The fourth group (Clause 9.4) has no possibility of a "coupon" strategy.

ISO and IEC draw attention to the fact that it is claimed that compliance with this document may involve the use of the following patents and their counterparts in other countries.

US 4 748 668 issued 1988-05-31, Inventors: A. Shamir and A. Fiat,

US 4 995 082 issued 1991-02-19, Inventor: C.P. Schnorr,

US 5 140 634 issued 1992-08-18, Inventors: L.C. Guillou and J-J. Quisquater,

EP 0 311 470 issued 1992-12-16, Inventors: L.C. Guillou and J-J. Quisquater,

EP 0 666 664 issued 1995-02-02, Inventor: M. Girault,

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 applications 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 overleaf.

News Digital Systems Ltd. Stoneham Rectory Stoneham Lane Eastleigh, Hampshire SO50 9NW, UK	US 4 748 668
RSA Security Inc. Attention General Counsel 174 Middlesex Turnpike Bedford, MA 01730, USA	US 4 995 082
France Telecom R&D 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
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
France Telecom claims that Patent Applications are pending in relation to Clauses 6 (GQ2) and 8 (GPS2). The Patent numbers will be provided when available. ISO/IEC will then request the appropriate statement.	

Information technology — Security techniques — Entity authentication —

Part 5:
Mechanisms using zero-knowledge techniques

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using zero-knowledge techniques.

— Clause 5 specifies mechanisms (already present in the first edition, ISO/IEC 9798-4:1999) based on identities and providing unilateral authentication. They have been repaired after the withdrawal of ISO/IEC 9796:1991.

— Clause 6 specifies mechanisms (inserted in this second edition) based on integer factorization and providing unilateral authentication.

— Clauses 7 and 8 specify mechanisms based on discrete logarithms with respect to numbers that are either prime (see Clause 7, mechanisms already present in the first edition) or composite (see Clause 8, mechanisms inserted in the second edition), and providing unilateral authentication.

— Clause 9 specifies mechanisms based on asymmetric encipherment systems and providing either unilateral (see 9.3, mechanisms already present in the first edition), or mutual (see 9.4, mechanisms inserted in the second edition) authentication.

The verifier associates the correct verification key with the claimant by any appropriate procedure, for example, by retrieving it from a certificate. Such procedures are outside the scope of this part of ISO/IEC 9798.

To identify each mechanism, Annex A specifies object identifiers in accordance with ISO/IEC 8825-1.

These mechanisms are constructed using the principles of zero-knowledge techniques, but they will not be zero-knowledge according to the strict definition sketched in Annex B for every choice of parameters.

Annex C compares the mechanisms and provides guidance on parameter choices.

Annex D provides numerical examples.

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 8825-1:2002, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

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

3 Terms and definitions

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

3.1
accreditation exponent
secret number related to the verification exponent and used in the production of private numbers

3.2
adaptation parameter
public number specific to the modulus and used in the definition of public numbers in the GQ2 mechanisms

3.3
asymmetric cryptographic technique
cryptographic technique that uses two related operations: a public operation defined by a public data item, key or number, and a private operation defined by a private data item, key or number (the two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation)

3.4
asymmetric encipherment system
system based on asymmetric cryptographic techniques whose public operation is used for encipherment and whose private operation is used for decipherment

3.5
asymmetric pair
two related data items, keys or numbers, where the private data item defines a private operation and the public data item defines a public operation

3.6
challenge
procedure parameter used in conjunction with secret parameters to produce a response

3.7
claimant
entity whose identity can be authenticated, including the functions and the private data necessary to engage in authentication exchanges on behalf of a principal

3.8
claimant parameter
public data item, number or bit string, specific to a given claimant within the domain

3.9
decipherment
reversal of a corresponding encipherment
[ISO/IEC 9798-1]

3.10
domain
collection of entities operating under a single security policy, e.g., public key certificates created by a single certification authority, or by a collection of certification authorities using the same security policy

3.11
domain parameter
public number, or function, agreed and used by all entities within the domain

3.12
encipherment
reversible operation by a cryptographic algorithm converting data into ciphertext, so as to hide the information content of the data

3.13
entity authentication
corroboration that an entity is the one claimed
[ISO/IEC 9798-1]

3.14
exchange multiplicity parameter
number of exchanges of information involved in one instance of an authentication mechanism

3.15
hash-function
function that maps strings of bits to fixed-length strings of bits, satisfying the following two properties:
— for a given output, it is computationally infeasible to find an input that maps to this output;
— it is computationally infeasible to find two distinct inputs that map to the same output
[ISO/IEC 10118-1]

3.16
identification data
set of public data items (e.g., an account number, an expiry date and time, a serial number, etc.) assigned to an entity and used to identify it

3.17
mutual authentication
entity authentication that provides both entities with assurance of each other's identity
[ISO/IEC 9798-1]

3.18
number
natural integer, i.e., a non-negative integer

3.19
pair multiplicity parameter
number of asymmetric pairs of numbers involved in one instance of an authentication mechanism

3.20
private key or private number
that data item, key or number, of an asymmetric pair, that shall be kept secret and should only be used by a claimant in accordance with an appropriate response formula, thereby establishing its identity

3.21
procedure parameter
public data item involved with a transient value in one instance of an authentication mechanism, e.g., witness, challenge, response

3.22
public key or public number
that data item, key or number, of an asymmetric pair, that can be made public and shall be used by every verifier for establishing the claimant's identity

3.23
random number
time variant parameter whose value is unpredictable
[ISO/IEC 9798-1]

3.24
response
procedure parameter produced by the claimant, and processed by the verifier for checking the identity of the claimant

3.25
secret parameter
number or bit string that does not appear in the public domain, only used by a claimant, e.g., a private number

3.26
token
message consisting of data fields relevant to a particular communication and which contains information that has been produced using a cryptographic technique

3.27
unilateral authentication
entity authentication that provides one entity with assurance of the other's identity but not vice versa
[ISO/IEC 9798-1]

3.28
verification exponent
public number used as exponent by the claimant and the verifier

3.29
verifier
entity including the functions necessary for engaging in authentication exchanges on behalf of an entity requiring an entity authentication

3.30
witness
procedure parameter that provides evidence of the claimant's identity to the verifier

4 Symbols and abbreviated terms

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

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

NOTE By definition, the Jacobi symbol of any positive integer *a* with respect to any odd positive composite integer *n* is the product of the Legendre symbols of *a* with respect to each prime factor of *n* (repeating the Legendre symbols for the repeated prime factors). The Jacobi symbol [10, 13] can be efficiently computed without knowledge of the prime factors of *n*.

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

NOTE By definition, the Legendre symbol of any positive integer *a* with respect to any odd positive prime integer *p* is set equal to $a^{(p-1)/2} \bmod p$. This means that $(a \mid p)$ is zero if *a* is a multiple of *p*, and either +1 or –1 otherwise, depending on whether or not *a* is a square modulo *p*.

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

NOTE The binary representation of a number *A* as a string of $|A|$ bits is straightforward. For representing a number *A* as a string of α bits with $\alpha > |A|$, $\alpha - |A|$ bits set to 0 are appended on the left of the $|A|$ bits.

$\lfloor A \rfloor$ the greatest integer that is less than or equal to the real number *A*

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

CRT Chinese Remainder Theorem

d challenge (procedure parameter)

D response (procedure parameter)

f	number of prime factors
gcd(a, b)	the greatest common divisor of the two integers a and b
G, G_i	public number (domain parameter)
$G(A)$, $G_i(A)$	public number (claimant parameter)
h	hash-function
$\|h\|$	bit length of the hash-code produced by the hash-function h
H, HH	hash-codes
$Id(A)$	identification data (claimant parameter)
$Id_i(A)$	part of the identification data (claimant parameter)
j mod n	the unique integer i from {0, 1, … n–1} so that n divides $j – i$
j mod* n	the unique integer i from {0, 1, … (n–1)/2} so that n divides either $j – i$ or $j + i$
lcm(a, b)	the least common multiple of the two integers a and b
m	pair multiplicity parameter (domain parameter)
n	composite modulus (domain parameter)
$n(A)$	composite modulus (claimant parameter)
p_1, p_2 …	prime factors of the modulus in ascending order, i.e. $p_1 < p_2 <$ … (secret parameters)
Q, Q_i	private number (secret parameter)
r	fresh random number or fresh string of random bits (secret parameter)
v	verification exponent (domain parameter)
W	witness (procedure parameter)
'XY'	notation using the hexadecimal digits '0' to '9' and 'A' to 'F', equal to XY to the base 16
α	modulus size in bits, i.e., $2^{\alpha-1} \leq$ modulus $< 2^{\alpha}$, also denoted $\|$modulus$\|$ (domain parameter)
δ	length of fresh strings of random bits for representing challenges (domain parameter)
ρ	length of fresh strings of random bits for representing random numbers (domain parameter)
{3, 5, 6}	set of the integers 3, 5 and 6

For the purposes of clause 5 (identity-based mechanisms), the following symbols and abbreviated terms apply.

F	bit string
t	exchange multiplicity parameter (domain parameter)
u	accreditation exponent with respect to the modulus (secret parameter)

u_j accreditation exponent with respect to the prime factor p_j (secret parameter)

For the purposes of clause 6 (integer factorization based mechanisms), the following symbols and abbreviated terms apply.

b adaptation parameter (specific to the modulus)

D_j response component with respect to the prime factor p_j (secret parameter)

g_i basic number (domain parameter)

$g_i(A)$ basic number (claimant parameter)

k security parameter (domain parameter)

$Q_{i,j}$ private component with respect to the basic number g_i and the prime factor p_j (secret parameter)

r_j fresh random number with respect to the prime factor p_j (secret parameter)

u_j accreditation exponent with respect to the prime factor p_j (secret parameter)

W_j witness component with respect to the prime factor p_j (secret parameter)

For the purposes of clause 7 (mechanisms based on discrete logarithms with respect to prime numbers), the following symbols and abbreviated terms apply.

g base of the discrete logarithms (domain parameter)

p modulus (domain parameter)

q prime number (domain parameter)

For the purposes of clause 8 (mechanisms based on discrete logarithms with respect to composite numbers), the following symbols and abbreviated terms apply.

g base of the discrete logarithms (domain parameter)

$g(A)$ base of the discrete logarithms (claimant parameter)

σ number of bits for private numbers in the first mode (domain parameter)

For the purposes of clause 9 (mechanisms based on asymmetric encipherment systems), the following symbols and abbreviated terms apply.

P_A public operation, i.e., encipherment (claimant parameter)

S_A private operation, i.e., decipherment (secret parameter)

x private RSA exponent (secret parameter)

5 Mechanisms based on identities

5.1 Security requirements for the environment

These mechanisms enable a verifier to check that a claimant knows private number(s) that are related to identification data by a verification key.

NOTE These mechanisms implement schemes due either to Fiat and Shamir [4] and denoted FS, or to Guillou and Quisquater [8] and denoted GQ1.

Within a given domain, the following requirements shall be satisfied.

1) Domain parameters shall be selected, which will govern the operation of the mechanism. They include a hash-function, e.g., one of the functions specified in ISO/IEC 10118-3. The selected parameters shall be made known in a reliable manner to all entities within the domain.

2) Every claimant shall be equipped with a modulus that is either a domain parameter or a claimant parameter. Each number used as modulus is set equal to the product of two or more distinct prime factors so that knowledge of its value shall not feasibly enable any entity to deduce its prime factors, where feasibility is defined by the context of use of the mechanism.

   — If the modulus is a domain parameter, then it is denoted n. A trusted authority has selected it and only this authority can use the corresponding prime factors. The authority guarantees the identities of every claimant within the domain.

   NOTE For example, a card issuer has a modulus. A delegated entity signs identification data for issuing smart cards; it uses the issuer's prime factors. In each card, the delegated entity stores appropriate identification data and private number(s). During its life, the card uses its private number(s) in accordance with an identity-based mechanism.

   — If the modulus is a claimant parameter, then it is denoted $n(A)$. A principal has selected it and the corresponding prime factors are the principal's long-term secret. For each session, the principal creates a claimant. The claimant uses private number(s) as a short-term secret.

   NOTE For example, in a local area network, an authority supervises each login operation within the domain and manages a directory where every verifier can obtain a trusted copy of a modulus for each principal.
   — During each login operation, i.e., when a computer opens a session, it uses a principal's prime factors for a "single-sign-on" of session identification data including identifier, expiry date and time, rights, etc.
   — During the session, the computer cannot use the prime factors because it does not know them any more. It uses the private number(s) in accordance with an identity-based mechanism. The private numbers only last for a few hours: their utility disappears after the session.

3) Every claimant shall be provided with identification data and with one or more private numbers by some means. In this context, the identification data is a string of bits, nor all equal, that uniquely and meaningfully identifies the claimant in accordance with an agreed convention.

   NOTE The presence of an expiry date and time in the identification data enforces their expiry; the presence of a serial number simplifies their revocation.

4) Every verifier shall obtain a trusted copy of the correct modulus of the claimant.

   NOTE The exact means by which the verifier obtains a trusted copy of the correct modulus is beyond the scope of this document. This may, for example, be achieved by the use of public-key certificates or by some other environment-dependent means.

5) Every claimant and every verifier shall have the means to produce random numbers.

5.2 Key production

5.2.1 Asymmetric key pair

A verification exponent, a pair multiplicity parameter and an exchange multiplicity parameter shall be selected. Unless otherwise specified, they are domain parameters respectively denoted v, m and t.

— Certain values of v, such as the prime numbers 2, 257, $2^{16}+1$, $2^{32}+15$, $2^{36}+2^{13}+1$ and $2^{40}+15$, have some practical advantages.

— The value of m shall be at most eight if $v = 2$ and set equal to one if v is an odd prime.

— The value of $v^{-m \times t}$ fixes a mechanism security level (see C.1.4). A value from 2^{-8} to 2^{-40} is appropriate for most applications.

A number, denoted α, fixes the modulus size in bits, i.e., $2^{\alpha-1} <$ modulus $< 2^{\alpha}$, in accordance with the context of use of the mechanism (for further details, see C.1.1). It is a domain parameter.

The authority or the principal shall keep secret two or more distinct large prime factors denoted p_1, p_2 … in ascending order, the product of which is the modulus.

- If $v = 2$ (the Rabin scheme), there shall be only two prime factors (i.e., $f = 2$), both congruent to 3 mod 4, but not congruent to each other mod 8.
- If v is an odd prime (the RSA scheme), there may be more than two prime factors. For each prime factor p_j, $p_j - 1$ shall be co-prime to v.

If α is a multiple of the number of prime factors, denoted f, then the bit size of each prime factor shall be α / f (for further details, see C.1.2). The modulus is set equal to either $p_1 \times p_2$ if $v = 2$, or $p_1 \times ... \times p_f$ if v is odd. In accordance with the second requirement in 5.1, the modulus is either a domain parameter denoted n, or a claimant parameter denoted $n(A)$.

With respect to each prime factor p_j, an accreditation exponent, denoted u_j, is set equal to the least positive integer so that $u_j \times v + 1$ is a multiple of either $(p_j - 1)/2$ if $v = 2$, or $p_j - 1$ if v is an odd prime.

With respect to the modulus, an accreditation exponent, denoted u, is set equal to the least positive integer so that $u \times v + 1$ is a multiple of either $\text{lcm}(p_1 - 1, p_2 - 1)/2$ if $v = 2$, or $\text{lcm}(p_1 - 1, \ldots p_f - 1)$ if v is an odd prime.

5.2.2 Asymmetric pair(s) of numbers

5.2.2.1 Case where $v = 2$

The identification data $Id(A)$ shall be converted into m parts by appending sixteen bits representing the numbers 1 to m, namely '0001', '0002', and so on, in turn to the string $Id(A)$.

$$Id_x(A) = Id(A) \,||\, \text{'000X'}$$

NOTE The mechanism below derives from the first format mechanism specified in ISO/IEC 14888-2 [21], known as PSS (PSS reads Probabilistic Signature Scheme) and due to Bellare and Rogaway [1].

For converting each part, from $Id_1(A)$ to $Id_m(A)$, into a string of α bits, denoted F_1 to F_m, the following computational steps are performed.

1) The string $Id_x(A)$ shall be hashed to obtain a hash-code denoted H_x.

$$H_x = h(Id_x(A))$$

2) A string of $(64 + |h|)$ bits is constructed from left to right by concatenating 8 octets set to '00' and the hash-code H_x. This string shall be hashed to obtain a hash-code denoted HH_x.

$$HH_x = h(\text{'00000000 00000000'} \,||\, H_x)$$

3) Named a mask, a string of $(\alpha - |h| - 8)$ bits is constructed from the hash-code HH_x. The procedure makes use of two variables: a bit string of variable length, denoted *String*, and a 32-bit counter, denoted *Counter*.
   a) Set *String* to the empty string.
   b) Set *Counter* to 0.
   c) Replace *String* by *String* || $h(HH_x$ || *Counter*).
   d) Replace *Counter* by *Counter* + 1.
   e) If $|h| \times$ *Counter* $< \alpha - |h| - 8$, then go to step c.

   $Mask_x$ equals the leftmost $(\alpha - |h| - 8)$ bits of *String* where the leftmost bit has been forced to 0.

4) A string denoted F_x is constructed from left to right by concatenating the $(\alpha - |h| - 8)$ bits of the mask where the rightmost bit has been reversed, the $|h|$ bits of the hash-code HH_x and one octet set to 'BC'.

$$F_x = \text{Format}(Id_x(A)) = (Mask_x \oplus (000 \ldots 000 \,||\, 1)) \,||\, HH_x \,||\, \text{'BC'}$$

A public number denoted $G_x(A)$ is derived from the number represented by the bit string F_x (also denoted F_x, this number is even, non-zero and less than the modulus), as follows.

— If the Jacobi symbol $(F_x \mid n)$ is +1, then $G_x(A) = F_x$.

— If the Jacobi symbol $(F_x \mid n)$ is –1, then $G_x(A) = F_x / 2$.

The authority or the principal shall provide claimant A with m private numbers denoted Q_1 to Q_m. The private number denoted Q_x is set equal to the u-th modular power of the public number $G_x(A)$.

$$Q_x = G_x(A)^{\,u} \text{ (mod* either } n \text{ or } n(A))$$

NOTE 1 The CRT technique (see C.2.3) may be used for converting each public number into a private number.

— For each prime factor p_j, a component Z_j is set equal to $G_x(A)^{\,uj} \bmod p_j$.

— A CRT composition converts the set of components $\{Z_1, Z_2 \ldots\}$ into a number Z.

$$Q_x = Z \text{ (mod* either } n \text{ or } n(A))$$

NOTE 2 Each asymmetric pair of numbers verifies a relationship governed by the verification key.

$$G_x(A) \times Q_x^{\,2} \equiv 1 \text{ (mod* either } n \text{ or } n(A))$$

NOTE 3 Consequently, any number $G_x(A)$ or Q_x may be replaced by the modulus minus the number.

5.2.2.2 Case where v is an odd prime

NOTE The mechanism below derives from the first format mechanism specified in ISO/IEC 14888-2 [21], known as PSS (PSS reads Probabilistic Signature Scheme) and due to Bellare and Rogaway [1].

For converting the identification data $Id(A)$ into a string of α bits, denoted F, the following computational steps are performed.

1) The string $Id(A)$ shall be hashed to obtain a hash-code denoted H.

$$H = h(Id(A))$$

2) A string of $(64+|h|)$ bits is constructed from left to right by concatenating 8 octets set to '00' and the hash-code H. This string shall be hashed to obtain a hash-code denoted HH.

$$HH = h(\text{'00000000 00000000'} \,||\, H)$$

3) Named a mask, a string of $(\alpha - |h|)$ bits is constructed from the hash-code HH. The procedure makes use of two variables: a bit string of variable length, denoted *String*, and a 32-bit counter, denoted *Counter*.

   a) Set *String* to the empty string.

   b) Set *Counter* to 0.

   c) Replace *String* by *String* || h(*HH* || *Counter*).

   d) Replace *Counter* by *Counter* + 1.

   e) If $|h| \times Counter < \alpha - |h|$, then go to step c.

   The mask equals the leftmost $(\alpha - |h|)$ bits of *String* where the leftmost bit has been forced to 0.

4) A string denoted F is constructed from left to right by concatenating the $(\alpha - |h|)$ bits of the mask where the rightmost bit has been reversed and the $|h|$ bits of the hash-code HH.

$$F = \text{Format}(Id(A)) = (Mask \oplus (000 \ldots 000 \,||\, 1)) \,||\, HH$$

A public number, denoted $G(A)$, is set equal to the number represented by the bit string F (also denoted F, this number is non-zero and less than the modulus).

$$G(A) = F$$