INTERNATIONAL STANDARD

ISO/IEC 9798-5

First edition
1999-03-15

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 les techniques de connaissance du zéro

Reference number
ISO/IEC 9798-5:1999(E)

Contents

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. 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.

International Standard ISO/IEC 9798–5 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Sub-Committee SC27, *IT Security techniques*.

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*

Annexes A, B, C, D, E, and F of this part of ISO/IEC 9798 are for information only.

ISO and IEC draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 9798 may involve the use of patents as given in Annex E.

ISO and IEC take no position regarding 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 licences 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 addresses given in Annex E.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 9798 may be the subject of patent rights other than those identified in Annex E. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero knowledge techniques

1 Scope

This part of ISO/IEC 9798 specifies three entity authentication mechanisms using zero knowledge techniques. All the mechanisms specified in this part of ISO/IEC 9798 provide unilateral authentication. These mechanisms are constructed using the principles of zero knowledge, but they will not be zero knowledge according to the strict definition sketched in Annex A for all choices of parameters.

The first mechanism is said to be based on identities. A trusted accreditation authority provides each claimant with private accreditation information, computed as a function of the claimant's identification data and the accreditation authority's private key.

The second mechanism is said to be certificate-based using discrete logarithms. Every claimant possesses a public key, private key pair for use in this mechanism. Every verifier of a claimant's identity must possess a trusted copy of the claimant's public verification key; the means by which this is achieved is beyond the scope of this standard, but it may be achieved through the distribution of certificates signed by a Trusted Third Party.

The third mechanism is said to be certificate-based using an asymmetric encipherment system. Every claimant possesses a public key, private key pair for an asymmetric cryptosystem. Every verifier of a claimant's identity must possess a trusted copy of the claimant's public key; the means by which this is achieved is beyond the scope of this standard, but it may be achieved through the distribution of certificates signed by a Trusted Third Party.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 9796: 1991, *Information technology — Security techniques — Digital signature scheme giving message recovery.*

ISO/IEC 9798–1, *Information technology — Security techniques — Entity authentication mechanisms — Part 1: General.*

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

3 Definitions

For the purposes of this part of ISO/IEC 9798, the following definitions apply.

The following terms are defined in ISO/IEC 9798–1.

3.1 asymmetric cryptographic technique:

3.2 asymmetric encipherment system:

3.3 asymmetric key pair:

3.4 challenge:

3.5 claimant:

3.6 decipherment:

3.7 distinguishing identifier:

3.8 encipherment:

3.9 entity authentication:

3.10 private key:

3.11 public key:

3.12 public verification key:

3.13 random number:

3.14 token:

3.15 trusted third party:

3.16 unilateral authentication:

3.17 verifier:

The following term is defined in ISO/IEC 10118–1.

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

- it is computationally infeasible to find for a given output an input which maps to this output;
- it is computationally infeasible to find for a given input a second input which maps to the same output.

In addition the following definitions are used.

3.19 accreditation authority: entity trusted by all members of a group of entities for the purposes of the generation of private accreditation information.

3.20 accreditation multiplicity parameter: positive integer equal to the number of items of secret accreditation information provided to an entity by the accreditation authority.

3.21 exchange multiplicity parameter: positive integer used to determine how many times the exchange of entity authentication messages shall be performed in one instance of the authentication mechanism.

3.22 identification data: sequence of data items, including the distinguishing identifier for an entity, assigned to an entity and used to identify it.

NOTE — Examples of data items which may be included in the identification data include: an account number, expiry date, serial number, etc.

3.23 private accreditation exponent: value known only to the accreditation authority, and which is used in the production of claimants' private accreditation information. This value shall be kept secret. This value is related to the public accreditation verification exponent.

3.24 private accreditation information: private information provided to a claimant by an accreditation authority, and of which a claimant subsequently proves knowledge, thereby establishing the claimant's identity.

3.25 private decipherment transformation: decipherment transformation determined by an asymmetric encipherment system and the private key of an asymmetric key pair.

3.26 public accreditation verification exponent: value agreed by all members of a group of entities, and which, in conjunction with the modulus, determines the value of the private accreditation exponent.

3.27 public encipherment transformation: encipherment transformation determined by an asymmetric encipherment system and the public key of an asymmetric key pair.

3.28 redundant identity: sequence of data items obtained from an entity's identification data by adding redundancy using techniques specified in ISO/IEC 9796.

3.29 response: data item sent by the claimant to the verifier, and which the verifier can process to help check the identity of the claimant.

3.30 witness: data item which provides evidence of the claimant's identity to the verifier.

4 Symbols and notation

For the purposes of this part of ISO/IEC 9798 the following symbols and notation described in ISO/IEC 9798–1 apply.

A — The distinguishing identifier of entity A.

B — The distinguishing identifier of entity B.

$Y||Z$ — The result of the concatenation of the data items Y and Z in that order.

The following general symbols and notation are used.

d — A challenge.

D — A response.

h — A hash-function.

r — A random number.

$\lfloor x \rfloor$ — The largest integer which is not greater than the value x.

mod — If i is an integer and n is a positive integer, then $i \bmod n$ denotes the unique integer j which satisfies

a) $0 \leq j < n$, and

b) $i - j$ is an integer multiple of n.

In the context of the identity-based mechanism of clause 5, the following symbols and notation are used.

$C_{A1}, C_{A2}, \ldots, C_{Am}$ — Entity A's private accreditation information.

gcd — The greatest common divisor of two integers, i.e. $\gcd(a, b)$ represents the largest positive integer that is a divisor of both a and b.

$I_{A1}, I_{A2}, \ldots, I_{Am}$ — The identification data of entity A. I_{Ai} is the ith part of the identification data of entity A.

$J_{A1}, J_{A2}, \ldots, J_{Am}$ — The redundant identity of entity A. J_{Ai} is the ith part of the redundant identity of entity A.

k_s — An integer determined by the modulus n, and which determines the maximum bit-length of the parts of an entity's redundant identity.

lcm — The least common multiple of two integers, i.e. $\mathrm{lcm}(a, b)$ represents the smallest positive integer that is a multiple of both a and b.

m — The accreditation multiplicity parameter.

n — A modulus equal to the product of the prime numbers p and q.

p — A prime number used to calculate the modulus.

q — A prime number used to calculate the modulus.

t — The exchange multiplicity parameter.

u — The accreditation authority's private accreditation exponent.

v — The public accreditation verification exponent.

W — A witness.

mod* — If i is an integer and n is a positive integer, then $i \bmod^* n$ denotes the non-negative integer j equal to the smaller of the two values: $i \bmod n$ and $n - i \bmod n$. If i and j are two integers and n is a positive integer then $i \equiv j \pmod^* n$ if and only if $i \bmod^* n = j \bmod^* n$.

$(a|n)$ — The Jacobi symbol of the positive integer a with respect to the odd positive integer n.

NOTE — Let p be an odd prime and let a be a positive integer. The Legendre symbol of a with respect to p, written $(a|p)$, is defined by

$$(a|p) = a^{(p-1)/2} \bmod p.$$

When a is not a multiple of p, $(a|p)$ is either +1 or -1, depending on whether or not a is equal to the square of an integer modulo p. The Legendre symbol of multiples of p with respect to a prime p is zero.

Let n be an odd positive integer satisfying $n = pq$, where p and q are primes, and let a be a positive integer. The Jacobi symbol of a with respect to n, written $(a|n)$, is defined by

$$(a|n) = (a|p)(a|q).$$

The Jacobi symbol $(a|n)$ can be computed efficiently without knowledge of the prime factorisation of n, see [6] and [8].

In the context of the discrete logarithm based mechanism of clause 6, the following symbols and notation are used.

g — A positive integer which is the base of the discrete logarithms.

p — A prime number used as a modulus.

q — A prime number which is a factor of $p - 1$.

y_X — The public verification key for entity X.

z_X — The private authentication key for entity X.

In the context of the trusted public transformation based mechanism of clause 7, the following symbols and notation are used.

P_X — The public encipherment transformation for entity X.

S_X — The private decipherment transformation for entity X.

5 Mechanism based on identities

In this clause an entity authentication mechanism is specified which is based on the use of identities.

5.1 Specific requirements

In order to use the mechanism within a group of entities, the following steps shall be taken.

a) Every entity wishing to act as either a claimant or a verifier must have the means to generate random numbers.

b) An accreditation authority shall be appointed for the group of entities. This accreditation authority shall be trusted by all members of the group for the purposes of guaranteeing identities.

c) A number of parameters shall be selected, which will govern the operation of the entity authentication mechanism. The selected parameters shall be made known in a reliable manner to all members of the group of entities.

d) Every entity wishing to act as a claimant in the authentication mechanism must be provided with identification data by some means. In this context identification data is a string of bits of length limited by one of the parameters selected in step (c), and which uniquely and meaningfully identifies the entity according to an agreed convention.

e) Every entity wishing to act as a claimant in the authentication mechanism shall be issued with private accreditation information by the selected accreditation authority.

f) If the version of the mechanism using a hash-function is selected, all entities within the group must agree on the use of a specific hash-function (for example one of the functions specified in ISO/IEC 10118).

5.2 Parameter selection

The parameters to be selected are as follows.

a) The public accreditation verification exponent v. Certain values, such as 2, 3 and $2^{16}+1 = 65537$, have some practical advantages.

b) The modulus n. This positive integer shall be selected by the appointed accreditation authority. The value of n shall be equal to the product of two prime numbers p and q. The values of p and q shall be kept secret by the accreditation authority. The prime numbers p and q shall be chosen in such a way that knowledge of their product n shall not feasibly enable any entity to deduce them, where feasibility is defined by the context of use of the authentication mechanism.

The values of p and q shall satisfy the following constraints:

— if v is odd, then $\gcd(p-1, v) = \gcd(q-1, v) = 1$, and

— if v is even, then $\gcd((p-1)/2, v) = \gcd((q-1)/2, v) = 1$, and $p - q$ shall not be a multiple of 8.

The choice of n determines the value of a further parameter, which is denoted by k_s, in the following way:

$$k_s = \lfloor \log_2(n) \rfloor.$$

In other words, a binary representation of n shall contain $k_s + 1$ bits.

The choice of n also determines the value of the accreditation authority's private accreditation exponent, denoted u, in the following way. The value u shall be set to the least positive integer such that $uv + 1$ is a multiple of

$$\begin{cases} \operatorname{lcm}(p-1, q-1) & \text{if } v \text{ is odd,} \\ \operatorname{lcm}(p-1, q-1)/2 & \text{if } v \text{ is even.} \end{cases}$$

c) The accreditation multiplicity parameter m. This positive integer shall be chosen in conjunction with the public accreditation verification exponent v and the exchange multiplicity t, and affects the level of security of the scheme.

d) The exchange multiplicity parameter t. This positive integer shall be chosen in conjunction with the public accreditation verification exponent v and the accreditation multiplicity m, and affects the level of security of the scheme.

NOTE 1 — Guidance on the choice of parameters for this mechanism is given in Annex B.

NOTE 2 — When $v = 2$ the mechanism becomes the Fiat-Shamir scheme, [3]. When $v > 2$, $m = 1$, and v is a prime the mechanism becomes the Guillou-Quisquater scheme, [5].

5.3 Identity selection

Each entity wishing to act as a claimant in this mechanism must be assigned identification data consisting of a sequence of m parts: $I_{A1}, I_{A2}, \ldots, I_{Am}$. Each part of the identification data shall contain at most $8\lfloor (k_s+3)/16 \rfloor$ bits.

The entity authentication mechanism will provide assurance to the verifier that the claimant is the entity which has been assigned this identification data.

NOTE 1 — This sequence of identification data parts could, for example, be constructed by assigning an entity a single identifying string of bits, and appending the binary representations of the numbers $1, 2, \ldots, m$ in turn to this string to obtain the values $I_{A1}, I_{A2}, \ldots, I_{Am}$. In such an approach, the binary representations of the numbers $1, 2, \ldots, m$ could conveniently all be made of the same length, by prefixing with zeros as necessary.

NOTE 2 — If the parts of an entity's identification data are longer than the maximum permissible length, then this can be dealt with by applying a hash-function to the identification data parts to obtain the values $I_{A1}, I_{A2}, \ldots, I_{Am}$. Examples of hash-functions can be found in ISO/IEC 10118.

NOTE 3 — Expiry of an entity's identification data can be enforced by the inclusion of an expiry date in the identification data. Revocation of an entity's identification data can be simplified by the inclusion of a serial number in the identification data.

5.4 Accreditation generation

To generate the private accreditation information for an entity A, the accreditation authority shall compute a sequence of m digital signatures $C_{A1}, C_{A2}, \ldots, C_{Am}$. More specifically, for every i $(1 \le i \le m)$, C_{Ai} shall be computed using the following procedure.

a) J_{Ai}, the ith part of the 'redundant identity' for A, shall be computed from I_{Ai}, the ith part of the identification data of A, by subjecting I_{Ai} to the first four steps of the signature process specified in ISO/IEC 9796, ('Padding', 'Extension', 'Redundancy' and 'Truncation and forcing'), using the specified value of k_s. The value obtained from this process, denoted IR, shall then be used to derive J_{Ai} in the following way.

— If v is odd then $J_{Ai} = IR$.

— If v is even and if $(IR|n) = +1$ then $J_{Ai} = IR$.

— If v is even and if $(IR|n) = -1$ then $J_{Ai} = IR/2$.

b) C_{Ai} shall be computed from J_{Ai} using the following formula:

$$C_{Ai} = (J_{Ai})^u \bmod^* n.$$

The private accreditation information supplied to entity A is equal to the computed signatures $C_{A1}, C_{A2}, \ldots, C_{Am}$.

Observe that

$$(C_{Ai})^v J_{Ai} \equiv 1 \pmod^* n$$

for every i $(1 \le i \le m)$.

5.5 Authentication exchange

This unilateral authentication mechanism involves the following exchanges of information between a claimant A and a verifier B, and enables B to check the identity of A. It is necessary for correct operation of the mechanism that B is provided with the claimed identification data of A, either appended to one of the information exchanges in the mechanism or by some other means.

One iteration of the authentication procedure is illustrated in figure 1. The bracketed numbers in the figure correspond to the steps of the exchange described in detail below.

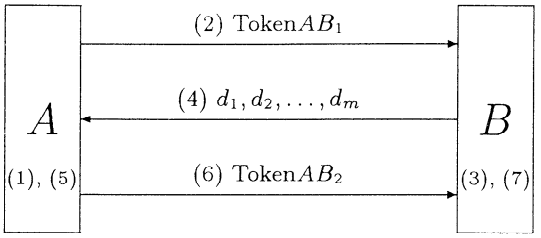

Figure 1 — Identity-based mechanism

The form of the first token (TokenAB_1), sent by the claimant to the verifier is either:

$$\text{Token}AB_1 = W$$

or

$$\text{Token}AB_1 = h(W||\text{Text})$$

where W is the witness, h is a hash-function, and Text is an optional text field. This text field is available for use in applications outside the scope of this part of ISO/IEC 9798 (it may be empty). See annex A of ISO/IEC 9798-1 for information on the use of text fields. If this text field is non-empty then B must have the means to recover the value of the text field; this may require A to send all or part of the text field with TokenAB_1 (see also Note 1 below).

The form of the second token (TokenAB_2), sent by the claimant to the verifier is:

$$\text{Token}AB_2 = D$$

where D is the response.

For each application of this mechanism the following authentication procedure shall be performed t times (where t is the exchange multiplicity parameter). The verifier B shall only accept the claimant A as valid if all t iterations of the procedure complete successfully.

(1) Entity A, who is equipped with private accreditation information $C_{A1}, C_{A2}, \ldots, C_{Am}$, chooses a random number r, subject to the restriction that r shall be an integer satisfying $1 \leq r \leq n-1$. This integer is kept secret by A. A now computes the witness W as

$$W = r^v \mod^* n.$$

(2) A sends TokenAB_1 to B. TokenAB_1 shall be equal to either W or $h(W||\text{Text})$.

(3) Having received TokenAB_1, B shall choose at random a sequence of integers $d_1, d_2, \ldots, d_m$, where each value d_i shall lie in the range 0 to $v-1$. This sequence of integers is the challenge.

(4) B sends the challenge $d_1, d_2, \ldots, d_m$ to A.

(5) On receipt of the challenge $d_1, d_2, \ldots, d_m$, A shall compute the response D from the (secret) value r and the private accreditation information $C_{A1}, C_{A2}, \ldots, C_{Am}$ as follows:

$$D = r \prod_{i=1}^{m} (C_{Ai})^{d_i} \mod^* n.$$

(6) A sends Token$AB_2 = D$ to B.

(7) On receipt of the response D, B shall perform the following computations.

(a) B checks that $0 < D < n/2$. If not then B shall reject A.

(b) B calculates $J_{A1}, J_{A2}, \ldots, J_{Am}$, the redundant identity of A, from the identification data $I_{A1}, I_{A2}, \ldots, I_{Am}$ of A, using the same process as specified in clause 5.4, step (a).

(c) B now computes the value W' using the following formula:

$$W' = D^v \prod_{i=1}^{m} (J_{Ai})^{d_i} \mod^* n.$$

(d) If W was sent in the first exchange of the procedure then B checks that the computed value W' is equal to the value of W sent in the first exchange of the procedure. Alternatively, if $h(W||\text{Text})$ was sent in the first exchange of the procedure then B first computes $h(W'||\text{Text})$ and then checks that $h(W'||\text{Text})$ is equal to the value of $h(W||\text{Text})$ sent in the first exchange of the procedure. If the check succeeds then this iteration of the mechanism is successful. Otherwise B rejects A.

NOTE 1 — Other information may be sent with any of the exchanges of any of the iterations of the authentication procedure. In particular note that information included within the identification data of A may be sent with TokenAB_1 in the first exchange of the first of the t iterations of the authentication procedure (step (2)). Such information might be used by B to help compute A's redundant identity and/or the value of the optional Text field.

NOTE 2 — It is important that A chooses the random value r by a process which guarantees that selected values are independent within the lifetime of the accreditation information. If, for example, the same value r is used twice, then a third party may be able to deduce part or all of the private accreditation information of A, and hence be able to impersonate A successfully.

NOTE 3 — The redundant identity $J_{A1}, J_{A2}, \ldots, J_{Am}$ for A can be computed at any stage by B, i.e. B need not wait until the

receipt of the response D before computing $J_{A1}, J_{A2}, \ldots, J_{Am}$. If B verifies A frequently using this mechanism, then B may cache the values $J_{A1}, J_{A2}, \ldots, J_{Am}$.

NOTE 4 — The t iterations of the procedure can be performed in parallel, i.e. in the first step A may choose t random numbers $r_1, r_2, \ldots, r_t$, compute t witnesses $W_1, W_2, \ldots, W_t$, send them simultaneously to B, and so on. If this 'parallel implementation' is adopted, the total number of message exchanges will be equal to three, regardless of the value of t.

NOTE 5 — The use of $h(W||\text{Text})$ instead of W in the first exchange of the procedure can achieve efficiency gains by reducing the number of bits in TokenAB_1.

NOTE 6 — It is recommended that the private accreditation information used in this mechanism be used only for the purposes of authentication, and should not be used for any other application (e.g. generation of digital signatures). If this recommendation is not followed then special care should be taken to prevent the verifier using the claimant as a 'signing oracle'; this could, for example, be achieved by requiring the challenge to be of a specially chosen form.

6 Certificate-based mechanism using discrete logarithms

In this clause an entity authentication mechanism is specified which uses discrete logarithms.

NOTE — This mechanism is known as the Schnorr scheme, [10].

6.1 Specific requirements

In order to use the mechanism within a group of entities, the following steps shall be taken.

a) Every entity wishing to act as either a claimant or a verifier must have the means to generate random numbers.

b) All entities within the group must agree on three positive integers p, q and g. The integer p must be chosen to be a prime number. Further q must be chosen to be a prime number which is also a factor of $p - 1$. Finally g must be chosen to be an element of order q modulo p, that is g must satisfy:

(i) $g^q \bmod p = 1$, and

(ii) $g \neq 1$.

The values p and g should be chosen so that, given an arbitrary integer i $(1 < i < q)$, finding an integer j (if one exists) such that $g^j \bmod p = i$ shall be computationally infeasible.

c) All entities within the group must agree on the use of a hash-function (for example one of the functions specified in ISO/IEC 10118).

d) Every entity wishing to act as a claimant must be equipped with an asymmetric key pair, selected as described below.

e) Every entity wishing to act as a verifier must be equipped with a means to obtain trusted copies of the public verification keys for the entities whose identities it is to verify.

NOTE — The exact means by which entities are provided with trusted copies of public verification keys is beyond the scope of this standard. This may, for example, be achieved by the use of public key certificates or by some other environment-dependent means.

6.2 Key selection

Each entity X wishing to act as a claimant in this mechanism must be equipped with an asymmetric key pair (y_X, z_X), where z_X (the private key) shall be an integer chosen to satisfy $0 < z_X < q$. The corresponding public verification key y_X shall be set equal to $g^{z_X} \bmod p$.

NOTE — Guidance on the choice of parameters for this mechanism is given in Annex B.

6.3 Authentication exchange

This unilateral authentication mechanism involves the following exchanges of information between a claimant A and a verifier B, and enables B to check the identity of A.

The authentication mechanism is illustrated in figure 2. The bracketed numbers in the figure correspond to the steps of the exchange described in detail below.

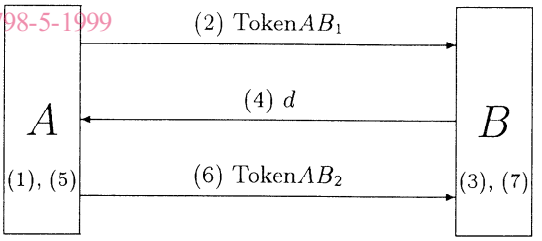

Figure 2 — Discrete logarithm based mechanism

The form of the first token (TokenAB_1), sent by the claimant to the verifier is either:

$$\text{Token}AB_1 = W$$

or

$$\text{Token}AB_1 = h(W||\text{Text})$$

where W is the witness, h is a hash-function, and Text is an optional text field. This text field is available for use in applications outside the scope of this part of ISO/IEC 9798 (it may be empty). See annex A of ISO/IEC 9798-1 for information on the use of text fields. If this Text field is non-empty then B must have the means to recover the value of Text; this may require A to send all or part of the Text field with TokenAB_1 (see also Note 1 below).