INTERNATIONAL STANDARD

ISO/IEC 29192-4

First edition
2013-06-01

Information technology — Security techniques — Lightweight cryptography

Part 4: **Mechanisms using asymmetric techniques**

Technologies de l'information — Techniques de sécurité — Cryptographie pour environnements contraints

Partie 4: Mécanismes basés sur les techniques asymétriques

Reference number
ISO/IEC 29192-4:2013(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 29192-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 29192 consists of the following parts, under the general title *Information technology — Security techniques — Lightweight cryptography*:

— *Part 1: General*

— *Part 2: Block ciphers*

— *Part 3: Stream ciphers*

— *Part 4: Mechanisms using asymmetric techniques*

Further parts may follow.

Introduction

This part of ISO/IEC 29192 specifies three lightweight mechanisms based on asymmetric cryptography. The three mechanisms have different functionality, different supporting infrastructures, and different performance profiles.

- cryptoGPS is a lightweight asymmetric identification scheme; in the cryptographic literature such schemes are generally described as interactive proofs of knowledge. While there are many types of such scheme, the computational costs for the prover when using cryptoGPS are relatively low. This is particularly the case since cryptoGPS is well-suited to an implementation strategy using what is often referred to as "coupons". These are, essentially, the results given by a modest off-line pre-computation, with coupons being used by the prover at each invocation of the cryptoGPS scheme. The resultant scheme, with the role of the prover being taken by a computationally restricted device such as an RFID tag, offers very useful performance trade-offs.

- ALIKE is an asymmetric mechanism for authentication and key exchange. Based on a variant of RSA, ALIKE offers a unilateral authentication and an additional functionality, i.e. secure key establishment. ALIKE offers implementation advantages when compared to conventional asymmetric solutions such as RSA.

- The third mechanism is an identity-based signature scheme. Hence a trusted third party is involved in the computation of distinct signature keys. This scheme offers implementation advantages over many other schemes in the cryptographic literature.

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.

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 the IEC that they are willing to negotiate licences either free of charge or 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:

France Telecom
38-40, rue du Général Leclerc, F-92794 Issy Les Moulineaux CEDEX 9, France

Gemalto SA
6, rue de La Verrerie, 92917 Meudon CEDEX, France

Agency for Science, Technology and Research
Agency for Science, Technology and Research c/o Exploit Technologies Pte Ltd,
30 Biopolis Street, #09-02 Matrix, Singapore 138671

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.

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

Information technology — Security techniques — Lightweight cryptography

Part 4: Mechanisms using asymmetric techniques

1 Scope

This part of ISO/IEC 29192 specifies three lightweight mechanisms using asymmetric techniques:

- a unilateral authentication mechanism based on discrete logarithms on elliptic curves;
- an authenticated lightweight key exchange (ALIKE) mechanism for unilateral authentication and establishment of a session key;
- an identity-based signature mechanism.

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

ISO/IEC 29192-1, *Information technology — Security techniques — Lightweight cryptography — Part 1: General*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29192-1 and the following apply.

3.1
asymmetric cryptographic technique
cryptographic technique that uses two related operations: a public operation defined by a public data item, and a private operation defined by a private data item

Note 1 to entry: The two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation.

[SOURCE: ISO/IEC 9798-5:2009, definition 2.3]

3.2
asymmetric pair
two related data items where the private data item defines a private operation and the public data item defines a public operation

[SOURCE: ISO/IEC 9798-5:2009, definition 2.5]

3.3
challenge
procedure parameter used in conjunction with secret parameters to produce a response

[SOURCE: ISO/IEC 9798-5:2009, definition 2.6]

3.4
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

[SOURCE: ISO/IEC 9798-5:2009, definition 2.7]

3.5
claimant parameter
public data item, number or bit string, specific to a given claimant within the domain

[SOURCE: ISO/IEC 9798-5:2009, definition 2.9]

3.6
collision-resistant hash-function
hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output

Note 1 to entry: computational feasibility depends on the specific security requirements and environment.

[SOURCE: ISO/IEC 10118-1:2000, definition 3.2]

3.7
coupon
pair of pre-computed numbers to be used only once

Note 1 to entry: One of the numbers shall be kept secret, and the other shall remain secret until the time of use.

[SOURCE: ISO/IEC 9798-5:2009, definition 2.8, modified]

3.8
domain
collection of entities operating under a single security policy

Note 1 to entry: For instance, public key certificates created either by a single certification authority, or by a collection of certification authorities using the same security policy.

[SOURCE: ISO/IEC 9798-5:2009, definition 2.11]

3.9
domain parameter
public key, or function, agreed and used by all entities within the domain

[SOURCE: ISO/IEC 9798-5:2009, definition 2.12]

3.10
entity authentication
corroboration that an entity is the one claimed

[SOURCE: ISO/IEC 9798-1:2010, definition 3.14]

3.11
exchange multiplicity parameter
number of exchanges of information involved in one instance of an authentication mechanism

[SOURCE: ISO/IEC 9798-5:2009, definition 2.15]

3.12
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

Note 1 to entry: Computational feasibility depends on the specific security requirements and environment.

[SOURCE: ISO/IEC 10118-1:2000, definition 3.5]

3.13
master secret key
secret data item

Note 1 to entry: Master secret key should only be used by the trusted server in accordance with the process of generation of signer private data.

3.14
private key
private data item of an asymmetric pair

Note 1 to entry: Private key shall be kept secret and should only be used by a claimant in accordance with an appropriate response formula, thereby establishing its identity.

[SOURCE: ISO/IEC 9798-5:2009, definition 2.21]

3.15
procedure parameter
transient public data item used in an instance of an authentication mechanism, e.g. a witness, challenge or response

[SOURCE: ISO/IEC 9798-5:2009, definition 2.22]

3.16
public key
public data item of an asymmetric pair, that can be made public and shall be used by every verifier for establishing the claimant's identity

[SOURCE: ISO/IEC 9798-5:2009, definition 2.23]

3.17
random number
time variant parameter whose value is unpredictable

[SOURCE: ISO/IEC 9798-1:2010, definition 3.29]

3.18
response
procedure parameter produced by the claimant, and processed by the verifier for checking the identity of the claimant

[SOURCE: ISO/IEC 9798-5:2009, definition 2.25]

3.19
secret parameter
number or bit string that does not appear in the public domain and is only used by a claimant

Note 1 to entry: For instance, a private key.

[SOURCE: ISO/IEC 9798-5:2009, definition 2.26]

3.20
sign
signature generation process that takes a message and a signing key of a signer to produce a signature

3.21
signer
entity with a unique bit string as an identity, including the functions and the private data necessary to engage in generation of a signature

3.22
signing key
secret data item given by the trusted server

Note 1 to entry: Signing key should only be used by a signer in accordance with the process of generation of a signature.

3.23
token
message consisting of data fields relevant to a particular communication and which contains information that has been produced using a cryptographic technique

[SOURCE: ISO/IEC 9798-5:2009, definition 2.27]

3.24
unilateral authentication
entity authentication which provides one entity with assurance of the other's identity but not vice versa

[SOURCE: ISO/IEC 9798-1:2010, definition 3.39]

3.25
verifier
entity including the functions necessary for engaging in authentication exchanges on behalf of an entity requiring an entity authentication or for engaging in verifying a signature of a given message and signer

[SOURCE: ISO/IEC 9798-5:2009, modified — Added the signature verification case]

3.26
verify
verification process that takes a message, a signature and an identity of a signer to output `accept` meaning the given signature is generated by the signer with the corresponding signing key, or `reject` otherwise

3.27
witness
procedure parameter that provides evidence of the claimant's identity to the verifier

[SOURCE: ISO/IEC 9798-5:2009, definition 2.31]

4 Symbols and abbreviated terms

For the purposes of this part of ISO/IEC 29192, the following symbols and abbreviated terms apply.

$|A|$ bit size of the number A if A is a non-negative integer (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 To represent a number A as a string of α bits with $\alpha > |A|$, $\alpha - |A|$ bits set to 0 are appended to the left of the $|A|$ bits.

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

$A[i]$ the i^{th}-bit of the number A, where $A[1]$ is the right-most bit and $A[|A|]$ is the left-most bit

$B \,||\, C$ bit string resulting from the concatenation of data items B and C in the order specified. In cases where the result of concatenating two or more data items is input to a cryptographic algorithm as part of an authentication mechanism, this result shall be composed so that it can be uniquely resolved into its constituent data strings, i.e. so that there is no possibility of ambiguity in interpretation. This latter property could be achieved in a variety of different ways, depending on the application. For example, it could be guaranteed by

(a) fixing the length of each of the substrings throughout the domain of use of the mechanism, or

(b) encoding the sequence of concatenated strings using a method that guarantees unique decoding, e.g. using the distinguished encoding rules defined in ISO/IEC 8825-1 [18]

D response (procedure parameter)

d challenge (procedure parameter)

E elliptic curve (domain parameter)

E_K block cipher encryption function with key K

e public exponent (domain parameter)

$f_0(u, x)$ $f_0(u, x) = 0 \,||\, x \,||\, \ldots \,||\, 0 \,||\, x \,||\, 0 \,||\, x^*$ where x^* represents the most significant bits of x (potentially no bits) required so that the length of $0 \,||\, x \,||\, \ldots \,||\, 0 \,||\, x \,||\, 0 \,||\, x^*$ is equal to u

$f_1(u, x)$ $f_1(u, x) = 1 \,||\, x \,||\, \ldots \,||\, 1 \,||\, x \,||\, 1 \,||\, x^*$ where x^* represents the most significant bits of x (potentially no bits) required so that the length of $1 \,||\, x \,||\, \ldots \,||\, 1 \,||\, x \,||\, 1 \,||\, x^*$ is equal to u

h hash-function

$|h|$ bit length of the hash-code produced by the hash-function h

HE padding function based on the block cipher E_K (domain parameter)

ID binary string that represents the identity or identification information

L bit length of the padding-code produced by the function HE (domain parameter)

m message

N composite modulus (domain parameter)

n order of the base point P (domain parameter)

$[n]P$ multiplication operation that takes a positive integer n and a point P on the curve E as input and produces as output another point Q on the curve E, where $Q = [n]P = P + P + \ldots + P$ is the sum of n occurrences of P. The operation satisfies $[0]P = 0_E$ (the point at infinity), and $[-n]P = [n](-P)$

P base point over the elliptic curve E (domain parameter)

p_1, p_2 … prime factors of the modulus in ascending order, i.e. $p_1 < p_2 < \ldots$ (secret parameters)

Q, Q_i private key (secret parameter)

q field size (domain parameter)

r fresh random number or fresh string of random bits (secret parameter)

T public point (domain parameter)

t master secret key (secret parameter)

u bit length of the key K in the block cipher encryption function E_K (domain parameter)

v bit length of a block-message in the block cipher encryption E_K (domain parameter)

W witness (procedure parameter)

w security parameter (domain parameter)

'X_1X_2 …' number whose hexadecimal representation is X_1X_2 …, where each X_i is equal to one of 0-9 and A-F

α modulus size in bits, i.e. $2^{\alpha-1} \le$ 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)

{a, b, c, …} set containing the elements a, b, c, …

5 Unilateral authentication mechanism based on discrete logarithms on elliptic curves

5.1 General

This mechanism, cryptoGPS – also called GPS in the earlier cryptographic literature –, is due to Girault, Poupard, and Stern [6]. The revised name is now used so as to avoid confusion with the physical location service GPS. cryptoGPS is a zero-knowledge identification scheme that provides unilateral entity authentication. Several variants of cryptoGPS are specified in ISO/IEC 9798-5 [21] and the version most suitable to constrained devices, along with some optimisations, is presented below.

5.2 Security requirements for the environment

The cryptoGPS mechanism enables a verifier to check that a claimant knows the elliptic curve discrete logarithm of a claimed public point with respect to a base point. A general framework for cryptographic techniques based on elliptic curves is given in ISO/IEC 15946-1.

NOTE 1 This mechanism implements the elliptic curve variant [5] of the cryptoGPS [6] scheme due to Girault, Poupard and Stern. It allows use of the so-called LHW (Low Hamming Weight) variant [4] particularly suitable for environments where the resources of the claimant are very low.

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