INTERNATIONAL STANDARD

ISO/IEC 29167-17

First edition
2015-06-01

Information technology — Automatic identification and data capture techniques —

Part 17:
Crypto suite cryptoGPS security services for air interface communications

Technologies de l'information — Techniques d'identification automatiques et de capture des données —

Partie 17: Services de sécurité par suite cryptographique cryptoGPS pour communications d'interface radio

Reference number
ISO/IEC 29167-17:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 31, *Automatic identification and data capture techniques*.

ISO/IEC 29167 consists of the following parts, under the general title *Information technology — Automatic identification and data capture techniques*:

- — *Part 1: Security services for RFID air interfaces*
- — *Part 10: Crypto suite AES-128 security services for air interface communications*
- — *Part 11: Crypto suite PRESENT-80 security services for air interface communications*
- — *Part 12: Crypto suite ECC-DH security services for air interface communications*
- — *Part 13: Crypto suite Grain-128A security services for air interface communications*
- — *Part 14: Crypto suite AES OFB security services for air interface communications*
- — *Part 16: Crypto suite ECDSA-ECDH security services for air interface communications*
- — *Part 17: Crypto suite cryptoGPS security services for air interface communications*
- — *Part 19: Crypto suite RAMON security services for air interface communications*

The following part is under preparation:

- — *Part 15: Crypto suite XOR security services for air interface communications*

Introduction

cryptoGPS is a lightweight asymmetric identification scheme that is suitable for RFID Tag authentication. While there are many types of such scheme, the computational costs for the Tag when using cryptoGPS are relatively low. This is particularly the case since cryptoGPS is well-suited to an implementation strategy using what is referred to as “coupons”. These are 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 offers very useful performance trade-offs.

This part of ISO/IEC 29167 specifies the security services of the cryptoGPS cryptographic suite that provides Tag authentication.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 29167 might involve the use of patents concerning radio-frequency identification technology given in the clauses identified below.

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

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

Orange
38-40, rue du General Leclerc **F-92794 Issy Les Moulineaux CEDEX 9**

The latest information on IP that might be applicable to this part of ISO/IEC 29167 can be found at www.iso.org/patents.

Information technology — Automatic identification and data capture techniques —

Part 17: Crypto suite cryptoGPS security services for air interface communications

1 Scope

This part of ISO/IEC 29167 defines the cryptoGPS cryptographic suite for the ISO/IEC 18000 air interfaces standards for radio frequency identification (RFID) devices. Its purpose is to provide a common crypto suite for security for RFID devices that might be referred by ISO committees for air interface standards and application standards.

This part of ISO/IEC 29167 defines a lightweight mechanism using asymmetric techniques and providing a unilateral authentication mechanism whose security is related to the difficulty of taking discrete logarithms on elliptic curves.

2 Conformance

2.1 Claiming conformance

To claim conformance with this part of ISO/IEC 29167, an Interrogator or Tag shall comply with all relevant clauses of this part of ISO/IEC 29167, except those marked as “optional”.

2.2 Interrogator conformance and obligations

To conform to this part of ISO/IEC 29167, an Interrogator shall

— implement the message and response formatting defined in this part of ISO/IEC 29167 and conform to the relevant part of ISO/IEC 18000.

To conform to this part of ISO/IEC 29167, an Interrogator might

— implement any subset of the parameters for message and response formatting defined in this part of ISO/IEC 29167.

To conform to this part of ISO/IEC 29167, the Interrogator shall not

— implement any command that conflicts with this part of ISO/IEC 29167, or

— require the use of an optional, proprietary, or custom command to meet the requirements of this part of ISO/IEC 29167.

2.3 Tag conformance and obligations

To conform to this part of ISO/IEC 29167, a Tag shall

— implement the message and response formatting defined in this part of ISO/IEC 29167 for the supported types and conform to the relevant part of ISO/IEC 18000.

To conform to this part of ISO/IEC 29167, a Tag might

- implement any subset of the parameters for message and response formatting defined in this part of ISO/IEC 29167.

To conform to this part of ISO/IEC 29167, a Tag shall not

- implement any command that conflicts with this part of ISO/IEC 29167, or
- require the use of an optional, proprietary, or custom command to meet the requirements of this part of ISO/IEC 29167.

3 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9798-5:2010, *Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques*

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

ISO/IEC 18000-3, *Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz*

ISO/IEC 18000-63, *Information technology — Radio frequency identification for item management — Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C*

ISO/IEC 19762 (all parts), *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

ISO/IEC 29167-1, *Information technology — Automatic identification and data capture techniques — Part 1: Security services for RFID air interfaces*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 (all parts) and the following apply.

4.1
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, 2.3]

4.2
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, 2.5]

4.3
challenge
procedure parameter used in conjunction with secret parameters to produce a response

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

4.4
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, 2.7]

4.5
claimant parameter
public data item, number or bit string, specific to a given claimant within the domain

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

4.6
commitment
public value used to engage a secret value without revealing it

Note 1 to entry: The commitment is used in a protocol so that a party cannot change a secret value after it has committed to it.

4.7
coupon
pre-computed number which shall be used only once

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

4.8
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, 2.11]

4.9
domain parameter
public key, or function, agreed and used by all entities within the domain

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

4.10
entity authentication
corroboration that an entity is the one claimed

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

4.11
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 two different input 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, 3.5]

4.12
private key
private data item 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

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

4.13
procedure parameter
transient public data item used in an instance of an authentication mechanism, e.g. a commitment, challenge, or response

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

4.14
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, 2.23]

4.15
random number
time variant parameter whose value is unpredictable

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

4.16
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, 2.25]

4.17
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, 2.26]

4.18
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, 3.39]

4.19
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]

4.20
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

4.21
witness

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

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

5 Symbols and abbreviated terms

5.1 Symbols

For the purposes of this part of ISO/IEC 29167, 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.
$A[i]$	i^{th}-bit of the number A, where $A[0]$ is the right-most bit and $A[\|A\|-1]$ is the left-most bit
$A[i:j]$	bit string made of the bits from the i^{th}-bit to the j^{th}-bit of the number A, where $i > j$
$B \|\| C$	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 [10]
Y	response (procedure parameter)
C	challenge (procedure parameter)
Δ	byte length of fresh strings of random bits for representing challenges (domain parameter)
δ'	bit length of fresh strings of random bits for representing challenges (domain parameter)
S_c	set of challenges c
Z	derived challenge (procedure parameter)
Ω	byte length of the derived challenge z (procedure parameter)
ω'	bit length of the derived challenge z (procedure parameter)
S_z	set of derived challenges z
E	elliptic curve (domain parameter)
TRUNC	truncation function; $\text{TRUNC}_k(\mathit{input})$ denotes the bitwise truncation of *input* to the k least significant (right-most) bytes
F	one-way function taking two inputs, a commitment X and a challenge c, and producing a derived challenge z
$\text{PRESENT}_K(B)$	encryption of the block B with the 128-bit key K, using the lightweight block cipher PRESENT
$\text{AES-}L_K(B)$	encryption of the block B with the L-bit key K, using the block cipher AES

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

N order of the base point P (domain parameter)

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

S private key (secret parameter)

Σ bit length of the secret key (domain parameter)

V public key (public parameter)

V byte length of the public key (domain parameter)

Q field size (domain parameter)

$r, \{r_i\}$ fresh random number or fresh string of random bits, or indexed set thereof (secret parameter)

P length of fresh strings of random bits for representing random numbers (domain parameter)

$X, \{X_i\}$ commitment, or indexed set thereof (procedure parameter)

X security parameter, length of a commitment X (domain parameter)

Θ security parameter (domain parameter)

Λ bit length of the signature of the public key (public parameter)

$\{a, b, c, \ldots\}$ set containing the elements $a, b, c, \ldots$

0^k string bit constructed with k zero bits

CCCC_b binary notation

CCCC_h hexadecimal notation

5.2 Abbreviated terms

CCR	Commitment Challenge Response
CS	Cryptographic Suite
CSI	Cryptographic Suite Identifier
ECDLP	Elliptic Curve Discrete Logarithm Problem
LHW	Low Hamming Weight
NTS	Non-transmissible Signature
RFU	Reserved for Future Use
TAM	Tag Authentication Method

6 Cipher introduction

This mechanism, cryptoGPS – called GPS in the earlier cryptographic literature – is due to Girault, Poupard, and Stern [3]. The name cryptoGPS is now used so as to avoid confusion with the physical location service. cryptoGPS is a zero-knowledge identification scheme that provides unilateral entity authentication. Several variants of cryptoGPS are specified in ISO/IEC 9798-5 and ISO/IEC 29192-4 [15] with the elliptic curve variant [2], along with some optimizations, being presented below.

cryptoGPS is a *public key*, or *asymmetric,* cryptographic mechanism for Tag authentication that offers the potential for lightweight implementation on the Tag and security that is related to the difficulty of solving the *elliptic curve discrete logarithm problem* (ECDLP).

Two variants of the authentication are described:

- The Commitment-Challenge-Response (CCR) variant. CCR schemes, such as cryptoGPS, have previously been proposed as lightweight solutions to the problem of Tag authentication.
- The Non-Transmissible Signature (NTS) variant. This variant is based on the cryptoGPS signature scheme and reduces the number of exchanges between the reader and the Tag.

In addition cryptoGPS can be used with a variety of implementation optimizations. These include:

a) the use of what are termed *coupons*, essentially a pre-computation of the form *(r, X)* that can be stored by the claimant and used at the time of authentication, and

b) the use of a pseudo-random number generator that can be used to re-generate the first component r of the coupons in optimization 1, and

c) the use of a cryptographic hash function that can be used to reduce the size of the second component X of the coupons in optimization 1, and

d) the use of bitwise truncation that can be used to further reduce the size of the second component X of the coupons in optimization 3, and

e) the use of what are termed *low hamming weight (LHW) challenges*, available only to the CCR variant, that provides a carefully constructed challenge space offering some computational efficiencies to the claimant. A challenge is said to be LHW if there are at least $\sigma - 1$ zero bits between any two consecutive one bits in its binary representation (where σ is the bit length of the private key s).

All of these optimizations are optional and they can be used in combination.

Issues such as the key infrastructure required to support the techniques described in this Cryptographic Suite are outside the scope of the document. They remain, nevertheless, important considerations when assessing the suitability of any Cryptographic Suite for a given application.

7 Parameter definitions

cryptoGPS allows 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.

Within a given domain the following requirements shall be satisfied.

a) Domain parameters that govern the operation of the mechanism shall be selected. The selected parameters shall be made available in a reliable manner to all entities within the domain.

b) Every claimant shall be equipped with the same elliptic curve E and a set of parameters, namely the field size q, a base point P over E, and n the order of point P. The curve and the set of parameters are either domain parameters or claimant parameters.

c) Each point P used as the base for elliptic curve discrete logarithms shall be such that, for any arbitrary point J of the curve, finding an integer k in $[0, n - 1]$ (if one exists) such that $J = [k]P$ is computationally infeasible, where feasibility is defined by the context of use of the mechanism.

d) Every claimant shall be equipped with a private key.