INTERNATIONAL STANDARD

ISO/IEC 29167-12

First edition
2015-05-15

Information technology — Automatic identification and data capture techniques —

Part 12: Crypto suite ECC-DH security services for air interface communication

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

Partie 12: Services de sécurité par suite cryptographique ECC-DH pour communications par interface radio

Reference number
ISO/IEC 29167-12:2015(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

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.

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*, Subcommittee SC 31, *Automatic identification and data capture*.

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 communication*

— *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 parts are under preparation:

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

Introduction

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly-known base point is computationally infeasible. The size of the elliptic curve determines the difficulty of the problem.

This part of ISO/IEC 29167 specifies the security services for an RFID Tag with an ECC-DH crypto suite based on the Diffie-Hellman key exchange algorithm. It specifies the details of a protocol and interface format for application with RFID Tags which provide unilateral authentication capability, based on the use of ECC. Although such Tags can operate in any frequency band legitimate for such applications, the main focus of this part of ISO/IEC 29167 is on externally-powered (also called "passive") Tags designed for the HF/UHF frequency bands, where the demands on low silicon footprint and power consumption are most stringent.

This part of ISO/IEC 29167 defines only Tag authentication for the ECC-DH cipher.

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 may involve the use of patents concerning radio-frequency identification and cryptographic technologies 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 ensured the ISO and IEC that they are willing to negotiate licenses under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC. Information on the declared patents may be obtained from:

Impinj, Inc.
701 N 34th Street, Suite 300 Seattle, WA 98103 USA

The latest information on IP that may 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 12: Crypto suite ECC-DH security services for air interface communication

1 Scope

This part of ISO/IEC 29167 defines the crypto suite for ECC-DH for the ISO/IEC 18000 air interfaces standards for radio frequency identification (RFID) devices. Its purpose is to provide a common crypto suite with Diffie-Hellmann-based authentication using ECC (elliptic curve cryptography) over binary fields for security for RFID devices that may be referred by ISO committees for air interface standards and application standards.

This part of ISO/IEC 29167 specifies a crypto suite for ECC-DH for air interface for RFID systems. The crypto suite is defined in alignment with existing air interfaces.

This part of ISO/IEC 29167 defines various authentication methods and methods of use for the cipher. A Tag and an Interrogator may support one, a subset, or all of the specified options, clearly stating what is supported.

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 mandatory commands 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 may

— implement any subset of the optional commands 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 mandatory commands 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 may

— implement any subset of the optional commands 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 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*

FIPS PUB 186-4, *Digital Signature Standard (DSS)*[1)]

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
Command (Message)
command that Interrogator sends to Tag with “Message” as parameter

4.2
Certificate
digitally signed statement binding a Public Key to an Identity

Note 1 to entry: The term “Certificate” is also known as “Public Key Certificate”.

4.3
double-word
bit string comprised of 32 bits

4.4
entropy
randomness collected by an operating system or application for use in cryptography or other uses that require random data

1) http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

4.5
isomorphism
one-to-one correspondence between the elements of two sets such that the result of an operation on elements of one set corresponds to the result of the analogous operation on their images in the other set

4.6
Message
part of the Command that is defined by the crypto suite

4.7
Reply (Response)
reply that Tag returns to the Interrogator with "Response" as parameter

4.8
weight
number of non-zero coefficients in the polynomial

4.9
Response
part of the Reply (stored or sent) that is defined by the crypto suite

4.10
X.509
ITU-T standard that defines what information should go into a certificate and describes the format

5 Symbols and abbreviated terms

5.1 Symbols

$xxxx_b$	binary notation of term "xxxx", where "x" represents a binary digit
$xxxx_h$	hexadecimal notation of term "xxxx", where "x" represents a hexadecimal digit
	In this part of ISO/IEC 29167 the bytes in the hexadecimal numbers are presented with the MSB at the left and the LSB at the right. The bit order per byte is also presented with the MSB at the left and the LSB at the right
	For example in "$ABCDEF_h$" the byte "AB" is the MSB and the byte "EF" is the LSB
||	Concatenation of syntax elements
	For example "123456_h" || "$ABCDEF_h$" results in "$123456ABCDEF_h$", where the byte "12" is the MSB and the byte "EF" is the LSB.
$()_x$	x-coordinate of an elliptic curve point
$()^{-1}$	the modular inverse of the polynomial defined within the braces, where the modulus is as indicated in the expression context
b(t)	polynomial basis representation of the curve parameter b (FIPS186-4)
cert(Q)	certificate of the public key Q
c(t)	check polynomial used in the EPIF Format
s(t)	such that $s^2(t) \bmod p(t) = b(t)$ i.e. the square root of b(t) in the field $GF(2^{163})$
E	elliptic curve

Field[a:b]	Selection from a string of bits in Field. Selection ranges from bit a till and including bit b from the bits of the string in Field, whereby Field[0] represents the least significant bit. For example Field[2:0] represents the selection of the three least significant bits of Field
G	base point on the elliptic curve B-163 defined in FIPS 186-4
GF(2)[t]/p(t)	$GF(2^n)$ represented as the field of polynomials modulo a polynomial p(t) of degree n
m(t)	the defining polynomial of the ring GF(2)[t]/m(t) used by the EPIF Format
N	degree of the polynomial p(t)
ϕ	order of the base point on the chosen curve; the bit length of ϕ is considered to be the key size (FIPS186-4 Notation: n)
p(t)	the field polynomial (FIPS186-4)
p'(t)	the defining polynomial of the isomorphic field GF(2)[t]/p'(t) used by the EPIF Format
Polstr()	binary transmission of the polynomial defined within the braces, highest possible degree bit first i.e. including leading zeros; hence if the maximum possible degree of a polynomial is 170, then 171 bits are transmitted i.e. coefficients of terms of degree 170 down to degree 0
Q	private key value of the Tag, a scalar in the range 2..ϕ-2
Q	public key of the Tag is the elliptic curve point; Q = qG
R	random value chosen by the Interrogator in the range 2..ϕ-2 (FIPS186-4)
P	isomorphism from GF(2)[t]/p(t) to GF(2)[t]/p'(t)
Σ	mapping from GF(2)[t]/p'(t) to GF(2)[t]/m(t)
Trace()	function which is a mapping from $GF(2^n)$ to GF(2); the quadratic equation $y^2 + y + \alpha = 0$ has a solution in $GF(2^n)$ when $Trace(\alpha) = 0$

5.2 Abbreviated terms

ECC	Elliptic Curve Cryptography
EPIF	Error-Protected Isomorphic Field
FIPS	Federal Information Processing Standard
GF(x)	Galois Field (with x elements)
HF	High Frequency (i.e. the frequency band 3MHz to 30 MHz)
NIST	(United States) National Institute of Standards and Technology
toEPIF	function which describes the transformation to the EPIF format

6 Introduction of the ECC-DH crypto suite

6.1 Core functionality

Elliptic curve cryptography has been the basis for many cryptographic protocols for authentication and key agreement. The oldest of these protocols is due to Diffie and Hellmann, and was originally described in Reference [1] as a method of key agreement between two parties performing computations in the multiplicative group of GF(p). This method and its analogous implementation using operations in a group of points on an elliptic curve defined over a finite field, are well known since the inception of public key cryptography, and are not described further here. Instead, attention is drawn to the specific idea of using this protocol for entity authentication, in which:

— One party (the proving entity or "prover") has a static public/private key-pair and a public key certificate which uses a digital signature to bind the public key with the name of the organization that produced the key-pair. In a real life application the certificate (with the digital signature) should be generated by a certification authority.

— The other party (the "verifier"), presents an ephemeral public key to the prover. The prover is required to perform an operation with the private key using this ephemeral public key as an input, and to return the result to the verifier.

— The verifier compares this result with that obtained from his own private key operation, using the ephemeral private key (effectively just a random number) and the prover's public key as an input.

The private key operation corresponds to multiplication of a point by the private key (a scalar). The public key corresponds to the multiplication of the private key (scalar) by a predetermined point on the curve, chosen as a domain parameter of the system. This protocol is illustrated by Figure 1 depicting an RFID system executing (an authentication protocol using) operations on a group of elliptic curve points.

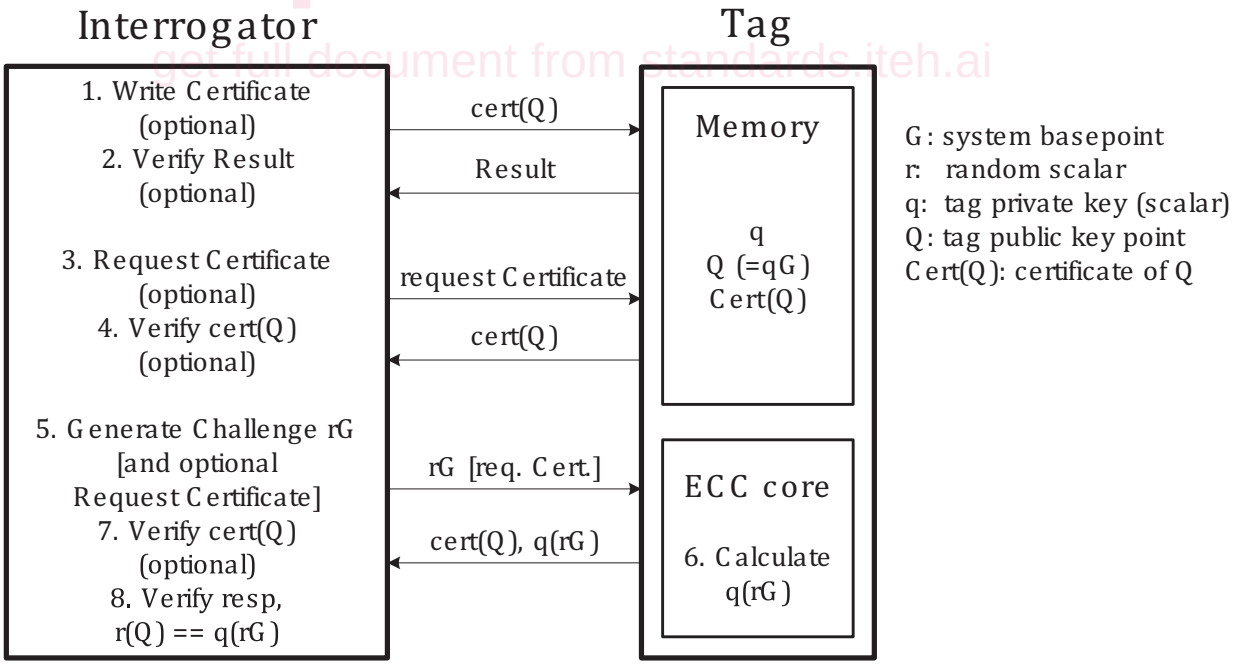

Figure 1 — Elliptic Curve static Diffie-Hellman authentication

In this protocol, the verifier (the Interrogator) first requests the public key certificate from the Tag and verifies if the certificate is valid. Then the Interrogator generates a ephemeral public key r and multiplies the system base point G by this number, and sends the resulting point rG to the prover (in this case the "Tag"). The Tag performs a multiplication of this point by its private key q and returns the result q(rG) to the Interrogator. The Interrogator then verifies that the private key q was really used by

checking that r(qG) = = q(rG) where (qG) = Q, the public key point of the Tag. The Interrogator must also verify that this public key is that of a valid Tag, and accordingly the Tag is also required (somewhere within the overall protocol) to present a certificate cert(Q), which is signed by a trusted authority who ensures the authenticity of the public key).

The mathematics of this protocol permits the elliptic curve computations to be performed using only the x-coordinates of points on the chosen curve (i.e. omitting the computations which involve the y-coordinate); this results in a lower requirement for computation, and is a well-known property of Diffie-Hellman protocols, identified in the early days of elliptic curve cryptography.

6.2 Design principles of the crypto suite

The design of the crypto suite is based on the following principles:

— The data exchanges between Tag and Interrogator are designed to minimize the processing and computation requirements on the Tag (for example, by using formats which avoid the need to perform modular inversion on the Tag). The exchange of elliptic curve points between Tag and Interrogator use x-coordinates only to reduce communication overhead and ease computation.

— The data exchanges between the Tag and the Interrogator facilitate simplest possible checking on the Tag that the x-coordinate of the point supplied to the Tag lies on the intended curve (and not on its twist), by sending the pair of values (x, (√b)/x) from the Interrogator to the Tag instead of sending the x and y coordinates of rG; the required check shall then be performed using only two Trace() computations and a single modular multiplication.

— The data exchanges between the Tag and the Interrogator include an integral integrity mechanism intended to facilitate integrity checking of cryptographic computations by both parties. In particular, protection of the computation which is supported. The integrity mechanism is specified in 7.2.

7 Parameter definitions

7.1 Elliptic curve parameters

This part of ISO/IEC 29167 uses Elliptic Curve Cryptography, more particularly it uses elliptic curves E defined over a binary extension field GF(2^n) where E is given by:

$$E: y^2 + xy = x^3 + ax^2 + b$$

The variables x and y in the above equation are the coordinates of an elliptic curve point and the coefficients a and b are elliptic curve parameters. The set of points fulfilling the equation together with a neutral point – the point at infinity – form a group under elliptic curve point addition. Elliptic Curve Cryptography uses a subgroup of this group generated by a generator G of order ϕ.

NOTE In this part of ISO/IEC 29167 the variable “a” has the constant value 1.

The binary extension field is usually represented as GF(2)[t]/p(t) where p(t) is a primitive polynomial of degree n; i.e. the elements of the field are represented as polynomials of degree less than n and operations are performed modulo p(t). For ease of notation the suffix (t) should be dropped when it is clear from the context that an element belongs to GF(2^n).

The authentication protocol defined in this part of ISO/IEC 29167 shall use the Elliptic Curve NIST B-163 whose parameters shall be used as defined in NIST FIPS 186-4.

NOTE please note that NIST FIPS 186–4 uses the variable n to denote the order of the base point (ϕ) and 2^m to denote the size of the binary field (2^n).