INTERNATIONAL STANDARD

ISO/IEC 29150

First edition
2011-12-15

Information technology — Security techniques — Signcryption

Technologies de l'information — Techniques de sécurité — Signcryptage

Reference number
ISO/IEC 29150:2011(E)

© ISO/IEC 2011

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

 © ISO/IEC 2011 – All rights reserved

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Symbols and notations 7

5 Finite fields and elliptic curves 8
5.1 Finite fields 8
5.2 Elliptic curves 9

6 Conversion functions 10
6.1 Bits and strings 10
6.2 Conversion between bit strings and integers 11
6.3 Conversion between finite field elements and integers/bit strings 11
6.4 Conversion between points on elliptic curves and bit strings 11

7 Cryptographic transformations 12
7.1 Introduction 12
7.2 Cryptographic hash functions 12
7.2.1 Standard cryptographic hash functions 12
7.2.2 Full domain cryptographic hash functions 12
7.2.2.1 General 12
7.2.2.2 Allowable full domain cryptographic hash function (FDH1) 13
7.3 Key derivation functions 13

8 General model for signcryption 13

9 Discrete logarithm based signcryption mechanism (DLSC) 15
9.1 Introduction 15
9.2 Specific requirements 15
9.3 System wide parameters 15
9.4 Key generation algorithm 16
9.5 Signcryption algorithm 16
9.6 Unsigncryption algorithm 17

10 Elliptic curve based signcryption mechanism (ECDLSC) 18
10.1 Introduction 18
10.2 Specific requirements 18
10.3 System wide parameters 18
10.4 Key generation algorithm 19
10.5 Signcryption algorithm 19
10.6 Unsigncryption algorithm 20

11 Integer factorization based signcryption mechanism (IFSC) 21
11.1 Introduction 21
11.2 Specific requirements 22
11.3 System wide parameters 22
11.4 Key generation algorithm 22
11.5 Signcryption algorithm 22
11.6 Unsigncryption algorithm 23

12 Encrypt-then-sign-based mechanism (EtS) 26
12.1 Introduction 26

© ISO/IEC 2011 – All rights reserved

12.2 Specific requirements **26**
12.3 Key generation algorithm **26**
12.4 Signcryption algorithm **27**
12.5 Unsigncryption algorithm **27**

Annex A (normative) **Object identifiers** **28**

Annex B (informative) **Security considerations** **30**

Annex C (informative) **Guidance on use of the mechanisms** **36**

Annex D (informative) **Examples** **40**

Bibliography **52**

 © ISO/IEC 2011 – All rights reserved

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.

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.

ISO/IEC 29150 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

© ISO/IEC 2011 – All rights reserved

Introduction

When data is sent from one place to another, it is often necessary to protect it in some way whilst it is in transit, e.g. against eavesdropping or unauthorized modification. Similarly, when data is stored in an environment to which unauthorized parties can have access, it is important to protect it against unauthorized access.

If the confidentiality of the data needs to be protected, e.g. against eavesdropping, then one solution is to use public key encryption, as specified in ISO/IEC 18033. Alternatively, if it is necessary to protect the data against unauthorized modification or forgery, then digital signatures, as specified in ISO/IEC 9796 and ISO/IEC 14888, can be used. If both confidentiality and unforgeability are required, then one possibility is to use both public key encryption and digital signature. Whilst these operations can be combined in many ways, not all combinations of such mechanisms provide the same security guarantees. As a result it is desirable to define in detail exactly how confidentiality and unforgeability mechanisms should be combined to provide the optimum level of security. Moreover, in some cases significant efficiency gains can be obtained by defining a single method of processing the data with the objective of providing both confidentiality and unforgeability.

In this International Standard, *signcryption mechanisms* are defined. These are methods for processing data to provide both confidentiality and unforgeability. These data processing methods typically involve either the use of an asymmetric encryption scheme and a digital signature scheme combined in a specific way or the use of a specially developed algorithm which fulfils both functions simultaneously.

The methods specified in this International Standard have been designed to maximise the level of security and provide efficient processing of data. All the mechanisms defined here have mathematical “proofs of security”, i.e. rigorous arguments supporting their security claims.

© ISO/IEC 2011 – All rights reserved

Information technology — Security techniques — Signcryption

1 Scope

This International Standard specifies four mechanisms for signcryption that employ public key cryptographic techniques requiring both the originator and the recipient of protected data to have their own public and private key pairs.

This International Standard is not applicable to infrastructures for management of public keys which are defined in ISO/IEC 11770-1 and ISO/IEC 9594.

NOTE 1 Signcryption mechanisms are defined ways of processing a data string with the following security objectives:

- **data confidentiality**, i.e. protection against unauthorized disclosure of data;
- **data integrity**, i.e. protection that enables the recipient of data to verify that it has not been modified;
- **data origin authentication**, i.e. protection that enables the recipient of data to verify the identity of the data originator;
- **data unforgeability**, i.e. protection against unauthorized modification of data, even by a recipient of the data.

These four security objectives are not necessarily mutually exclusive. The fourth objective, data unforgeability, in particular is a stronger notion of security that implies both data integrity and data origin authentication.

NOTE 2 Two of the mechanisms specified in this International Standard, namely mechanisms DLSC and ECDLSC, require the employment of system wide public key parameters for both the sender and the recipient of data. In a system where a multiple number of pairs of senders and recipients exist, the same system wide parameters are required to be used by all these users. The two remaining specified mechanisms, namely IFSC and EtS, do not require the use of such system wide public key parameters.

NOTE 3 In selecting the four signcryption mechanisms for inclusion in this International Standard from the large variety of such techniques published and in use, the same seven criteria as those stated in ISO/IEC 18033-1:2005, Annex A, have been followed. The exclusion of particular methods does not imply that those methods are insecure.

NOTE 4 This International Standard bears a conceptual similarity to ISO/IEC 19772[14] which specifies a number of mechanisms for authenticated encryption, that is, simultaneously achieving message integrity and confidentiality. Major differences between ISO/IEC 19772 and this International Standard include (1) mechanisms specified in ISO/IEC 19772 fall into the category of symmetric cryptographic techniques, whereas those specified in this International Standard are representatives of asymmetric cryptographic techniques; (2) while all mechanisms specified in ISO/IEC 19772 and this International Standard offer the capability of data integrity and origin authentication, mechanisms specified in this International Standard further offer the capability of data unforgeability, even by a recipient of the data.

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 9796-2:2010, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

© ISO/IEC 2011 – All rights reserved

ISO/IEC 9796-3:2006, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms*

ISO/IEC 14888-1:2008, *Information technology — Security techniques — Digital signatures with appendix — Part 1: General*

ISO/IEC 14888-2:2008, *Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms*

ISO/IEC 14888-3:2006, *Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*

ISO/IEC 18033-1:2005, *Information technology — Security techniques — Encryption algorithms — Part 1: General*

ISO/IEC 18033-2:2006, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

© ISO/IEC 2011 – All rights reserved