

First edition  
2010-05-01

---

---

**Information technology —  
Telecommunications and information  
exchange between systems — NFC  
Security —**

**Part 2:  
NFC-SEC cryptography standard using  
ECDH and AES**

*Technologies de l'information — Téléinformatique — Sécurité NFC —  
Partie 2: Norme de cryptographie NFC-SEC utilisant ECDH et AES*

---

---

Reference number  
ISO/IEC 13157-2:2010(E)



This is a preview of "ISO/IEC 13157-2:2010". [Click here to purchase the full version from the ANSI store.](#)

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2010

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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

This is a preview of "ISO/IEC 13157-2:2010". Click here to purchase the full version from the ANSI store.

## Contents

Page

Foreword .....	iv
Introduction.....	v
1 Scope .....	1
2 Conformance .....	1
3 Normative references .....	1
4 Terms and definitions .....	2
5 Conventions and notations .....	2
5.1 Concatenation.....	2
5.2 Hexadecimal numbers .....	2
6 Acronyms .....	2
7 General .....	3
8 Protocol Identifier (PID) .....	3
9 Primitives.....	3
9.1 Key agreement.....	4
9.2 Key Derivation Functions .....	5
9.3 Key Usage .....	5
9.4 Key Confirmation.....	6
9.5 Data Encryption .....	6
9.6 Data Integrity.....	7
9.7 Message Sequence Integrity .....	7
10 Data Conversions .....	7
10.1 Integer-to-Octet-String Conversion .....	7
10.2 Octet-String-to-Integer Conversion .....	7
10.3 Point-to-Octet-String Conversion .....	8
10.4 Octet-String-to-Point Conversion .....	8
11 SSE and SCH service invocation .....	8
11.1 Pre-requisites.....	9
11.2 Key Agreement .....	9
11.3 Key Derivation .....	10
11.4 Key Confirmation.....	11
12 SCH data exchange .....	12
12.1 Preparation.....	12
12.2 Data Exchange.....	12
Annex A (normative) AES-XCBC-PRF-128 and AES-XCBC-MAC-96 algorithms.....	14
Annex B (normative) Fields sizes.....	15
Annex C (informative) Informative references .....	16

## 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 13157-2 was prepared by Ecma International (as ECMA-386) and was adopted, under a special "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

ISO/IEC 13157 consists of the following parts, under the general title *Information technology — Telecommunications and information exchange between systems — NFC Security*:

- *Part 1: NFC-SEC NFCIP-1 security services and protocol*
- *Part 2: NFC-SEC cryptography standard using ECDH and AES*

This is a preview of "ISO/IEC 13157-2:2010". [Click here to purchase the full version from the ANSI store.](#)

## Introduction

The NFC Security series of standards comprise a common services and protocol standard and NFC-SEC cryptography standards.

This NFC-SEC cryptography standard specifies cryptographic mechanisms that use the Elliptic Curves Diffie-Hellman (ECDH) protocol for key agreement and the AES algorithm for data encryption and integrity.

This International Standard addresses secure communication of two NFC devices that do not share any common secret data ("keys") before they start communicating with each other.