

---

---

**Information technology — Security  
techniques — Lightweight cryptography**

Part 4:  
**Mechanisms using asymmetric  
techniques**

*Téchnologies de l'information — Techniques de sécurité —  
Cryptographie pour environnements contraints*

*Partie 4: Mécanismes basés sur les techniques asymétriques*



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2013

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested 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

# Contents

Page

Foreword .....	iv
Introduction.....	v
<b>1 Scope .....</b>	<b>1</b>
<b>2 Normative references .....</b>	<b>1</b>
<b>3 Terms and definitions .....</b>	<b>1</b>
<b>4 Symbols and abbreviated terms .....</b>	<b>4</b>
<b>5 Unilateral authentication mechanism based on discrete logarithms on elliptic curves.....</b>	<b>6</b>
<b>5.1 General .....</b>	<b>6</b>
<b>5.2 Security requirements for the environment.....</b>	<b>6</b>
<b>5.3 Key production .....</b>	<b>7</b>
<b>5.4 Unilateral authentication mechanism.....</b>	<b>8</b>
<b>6 Unilateral authenticated key exchange mechanism based on encryption.....</b>	<b>9</b>
<b>6.1 General .....</b>	<b>9</b>
<b>6.2 Security requirements for the environment.....</b>	<b>10</b>
<b>6.3 Key production .....</b>	<b>10</b>
<b>6.4 Unilateral authentication exchange.....</b>	<b>11</b>
<b>6.5 Session-key derivation .....</b>	<b>12</b>
<b>7 Identity-based signature mechanism .....</b>	<b>12</b>
<b>7.1 General .....</b>	<b>12</b>
<b>7.2 Security requirements for the environment.....</b>	<b>12</b>
<b>7.3 Key production .....</b>	<b>13</b>
<b>7.4 Sign.....</b>	<b>13</b>
<b>7.5 Verify.....</b>	<b>13</b>
<b>Annex A (normative) Object identifiers .....</b>	<b>14</b>
<b>Annex B (normative) Memory-Computation Trade-Off Technique .....</b>	<b>15</b>
<b>Annex C (informative) Numerical examples .....</b>	<b>16</b>
<b>C.1 cryptoGPS mechanism .....</b>	<b>16</b>
<b>C.1.1 Key production .....</b>	<b>16</b>
<b>C.1.2 Authentication exchange.....</b>	<b>16</b>
<b>C.2 ALIKE mechanism .....</b>	<b>18</b>
<b>C.2.1 Key production .....</b>	<b>18</b>
<b>C.2.2 Authentication exchange.....</b>	<b>18</b>
<b>C.2.3 Session-key derivation .....</b>	<b>19</b>
<b>C.3 Identity-based signature mechanism .....</b>	<b>19</b>
<b>C.3.1 Key production .....</b>	<b>19</b>
<b>C.3.2 Sign.....</b>	<b>20</b>
<b>C.3.3 Verify.....</b>	<b>21</b>
<b>Annex D (informative) Features .....</b>	<b>22</b>
<b>Bibliography.....</b>	<b>25</b>

## 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](http://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*