

Second edition
2006-09-15

Corrected version
2013-09-15

**Information technology — Security
techniques — Digital signature schemes
giving message recovery —**

**Part 3:
Discrete logarithm based mechanisms**

*Technologies de l'information — Techniques des sécurité — Schémas
de signature numérique rétablissant le message —*

Partie 3: Mécanismes basés sur les logarithmes discrets

Reference number
ISO/IEC 9796-3:2006(E)



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.

© ISO/IEC 2006

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

Contents

Foreword	v
Introduction.....	vi
1 Scope	1
2 Normative references.....	1
3 Terms and definitions	1
4 Symbols, notation and conventions.....	4
4.1 Symbols and notation.....	4
4.2 Conversion functions and mask generation functions.....	6
4.3 Legend for figures	6
5 Binding between signature mechanisms and hash-functions	7
6 Framework for digital signatures giving message recovery	7
6.1 Processes.....	7
6.2 Parameter generation process.....	8
6.3 Signature generation process.....	8
6.4 Signature verification process.....	9
7 General model for digital signatures giving message recovery	9
7.1 Requirements.....	9
7.2 Summary of functions and procedures	10
7.3 User key generation process	11
7.4 Signature generation process.....	11
7.5 Signature verification process.....	14
8 NR (Nyberg-Rueppel message recovery signature)	17
8.1 Domain parameter and user keys.....	17
8.2 Signature generation process.....	17
8.3 Signature verification process.....	18
9 ECNR (Elliptic Curve Nyberg-Rueppel message recovery signature).....	19
9.1 Domain parameter and user keys.....	19
9.2 Signature generation process.....	19
9.3 Signature verification process.....	20
10 ECMR (Elliptic Curve Miyaji message recovery signature).....	21
10.1 Domain parameter and user keys.....	21
10.2 Signature generation process.....	22
10.3 Signature verification process.....	23
11 ECAO (Elliptic Curve Abe-Okamoto message recovery signature)	23
11.1 Domain parameter	23
11.2 User keys.....	24
11.3 Signature generation process.....	24
11.4 Signature verification process.....	26
12 ECPV (Elliptic Curve Pintsov-Vanstone message recovery signature).....	27
12.1 Domain and user parameters	27
12.2 Signature generation process.....	28
12.3 Signature verification process.....	29
13 ECKNR (Elliptic Curve KCDSA/Nyberg-Rueppel message recovery signature).....	31
13.1 Domain parameter and user keys.....	31
13.2 Signature generation process.....	31
13.3 Signature verification process.....	32