

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

Part 3: Discrete logarithm based mechanisms

ICS 35.040

National foreword

This British Standard is the UK implementation of ISO/IEC 9796-3:2006.

The ISO corrected text [15 September 2013] incorporates the following editorial corrections:

- The year of publication has been removed from references to ISO/IEC 15946-1.
- The last paragraph of 6.2.1 has been modified and ISO/IEC 15946-5 has been added to Clause 2.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT — Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2006

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 82245 2

Amendments/corrigenda issued since publication

Date	Comments
28 February 2014	Implementation of ISO corrected text 15 September 2013