

Licensed copy: Welcome University of Michigan Library, The Regents of the University, Version correct as of 06/12/2019



BSI Standards Publication

IT Security techniques — Digital signatures with appendix

Part 3: Discrete logarithm based mechanisms

National foreword

This British Standard is the UK implementation of [ISO/IEC 14888-3:2018](#). It supersedes [BS ISO/IEC 14888-3:2016](#), which is withdrawn.

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.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 539 01614 7

ICS 35.030; 35.040.01

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 30 November 2018.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

**IT Security techniques — Digital
signatures with appendix —**

**Part 3:
Discrete logarithm based mechanisms**

*Techniques de sécurité IT — Signatures numériques
avec appendice —*

Partie 3: Mécanismes basés sur un logarithme discret