

BS ISO/IEC 9797-2:2011

Incorporating corrigendum September 2015



BSI Standards Publication

Information technology — Security techniques — Message Authentication Codes (MACs)

Part 2: Mechanisms using a dedicated hash-function

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO/IEC 9797-2:2011. It supersedes BS ISO/IEC 9797-2:2002 which is withdrawn.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 2015.

Published by BSI Standards Limited 2015

ISBN 978 0 580 91701 1

ICS 35.040

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 May 2011.

Amendments/corrigenda issued since publication

Date	Text affected
30 September 2015	Implementation of ISO corrected text 15 June 2011: corrections to subclauses 3.14, 6.3, 6.3.5 and 6.3.6