



BSI Standards Publication

Information security — Message authentication codes (MACs)

Part 2: Mechanisms using a dedicated hash-function

National foreword

This British Standard is the UK implementation of ISO/IEC 9797-2:2021, incorporating corrigendum November 2024. It supersedes BS ISO/IEC 9797-2:2011, which is withdrawn.

The start and finish of text introduced or altered by corrigendum is indicated in the text by tags. Text altered by ISO/IEC corrigendum November 2024 is indicated in the text by AC1 AC1.

The UK participation in its preparation was entrusted to Technical Committee IST/33/2, Cryptography and Security Mechanisms.

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

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 29153 7

ICS 35.030

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 June 2021.

Amendments/corrigenda issued since publication

Date	Text affected
31 December 2024	Implementation of ISO/IEC corrigendum November 2024