



BSI Standards Publication

IT Security techniques — Entity authentication

Part 2: Mechanisms using authenticated encryption

National foreword

This British Standard is the UK implementation of [ISO/IEC 9798-2:2019](#). It supersedes [BS ISO/IEC 9798-2:2008](#), which is withdrawn.

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 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 2019
Published by BSI Standards Limited 2019

ISBN 978 0 580 51051 9

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 2019.

Amendments/corrigenda issued since publication

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

**IT Security techniques — Entity
authentication —**

Part 2:
**Mechanisms using
authenticated encryption**

*Techniques de sécurité IT — Authentification d'entité —
Partie 2: Mécanismes utilisant le chiffrement authentifié*