

# Information technology — Security techniques — Authenticated encryption

ICS 35.040

## National foreword

This British Standard is the UK implementation of ISO/IEC 19772:2009, incorporating corrigendum September 2014.

The start and finish of text introduced or altered by corrigendum is indicated in the text by tags. Text altered by ISO/IEC corrigendum September 2014 is indicated in the text by AC1 AC1.

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.

The 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 July 2009

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

ISBN 978 0 580 86465 0

### Amendments/corrigenda issued since publication

| Date              | Comments                                             |
|-------------------|------------------------------------------------------|
| 30 September 2014 | Implementation of ISO/IEC corrigendum September 2014 |
|                   |                                                      |
|                   |                                                      |
|                   |                                                      |