INTERNATIONAL STANDARD ISO/IEC 9798-2:2008
TECHNICAL CORRIGENDUM 2

Published 2012-03-15

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Security techniques — Entity authentication —

Part 2: **Mechanisms using symmetric encipherment algorithms**

TECHNICAL CORRIGENDUM 2

Technologies de l'information — Techniques de sécurité — Authentification d'entité —

Partie 2: Mécanismes utilisant des algorithmes de chiffrement symétriques

RECTIFICATIF TECHNIQUE 2

Technical Corrigendum 2 to ISO/IEC 9798-2:2008 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page 4, Clause 5

Add the following after the last paragraph:

f) The secret authentication key used in implementations of any of the mechanisms specified in this part of ISO/IEC 9798 shall be distinct from keys used for any other purposes.

g) The data strings enciphered at various points in an authentication mechanism shall not be composed so that they could be interchanged.

NOTE This could be enforced by including the following elements in each enciphered data string.

— The object identifier as specified in Annex A, in particular identifying the ISO standard, the part number, and the authentication mechanism.

Published in Switzerland

- A constant that uniquely identifies the enciphered string within the mechanism. This constant may be omitted in mechanisms that include only one enciphered string.

The recipient of an enciphered data string shall verify that the object identifier and the constant identifying the enciphered data string within the mechanism are as expected.