INTERNATIONAL STANDARD ISO/IEC 9798-2:2008
TECHNICAL CORRIGENDUM 1

Published 2010-02-15

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 1

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

Partie 2: Mécanismes utilisant des algorithmes de chiffrement symétriques

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 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 3, Clause 4

Replace the definition of $X \| Y$ with the following text:

"The result of the concatenation of data items X and Y in the order specified. In cases where the result of concatenating two or more data items is encrypted as part of one of the mechanisms specified in this part of ISO/IEC 9798, this result shall be composed so that it can be uniquely resolved into its constituent data strings, i.e. so that there is no possibility of ambiguity in interpretation. This latter property could be achieved in a variety of ways, depending on the application. For example, it could be guaranteed by (a) fixing the length of each of the substrings throughout the domain of use of the mechanism, or (b) encoding the sequence of concatenated strings using a method that guarantees unique decoding, e.g. using the distinguished encoding rules defined in ISO/IEC 8825-1 [1].

NOTE Not only concatenated strings but ordered tuples are needed. Normally, the notation for ordered tuples is $[X_1,X_2,...,X_n]$."

Delete the NOTE from the last row of the table.

ICS 35.040 **Ref. No. ISO/IEC 9798-2:2008/Cor.1:2010(E)**

Published in Switzerland