INTERNATIONAL STANDARD ISO/IEC 9798-4:1999
TECHNICAL CORRIGENDUM 1

Published 2009-09-15

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 4:
Mechanisms using a cryptographic check function

TECHNICAL CORRIGENDUM 1

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

Partie 4: Mécanismes utilisant une fonction cryptographique de vérification

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 9798-4:1999 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page 1, Clause 3

Insert the following text at the end of this clause:

As defined in ISO/IEC 9798-1, $X||Y$ is used to mean 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 input to a cryptographic check function 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 different 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].

ICS 35.040 **Ref. No. ISO/IEC 9798-4:1999/Cor.1:2009(E)**

Published in Switzerland