INTERNATIONAL STANDARD ISO/IEC 9798-6:2005
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 6: **Mechanisms using manual data transfer**

TECHNICAL CORRIGENDUM 1

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

Partie 6: Mécanismes utilisant un transfert manuel de données

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 9798-6:2005 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page 3, Clause 5

Add the following list item at the end of this clause:

i) For mechanisms 3 and 4, the result of concatenating data items prior to the computation of a MAC shall have the following property. The concatenation 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 [13].

ICS 35.040 **Ref. No. ISO/IEC 9798-6:2005/Cor.1:2009(E)**

Published in Switzerland

Page 20, Bibliography

Add the following at the end of the bibliography:

[13] ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*