INTERNATIONAL STANDARD ISO/IEC 9798-2:2008
TECHNICAL CORRIGENDUM 3

Published 2013-02-15

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 3

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

Partie 2: Mécanismes utilisant des algorithmes de chiffrement symétriques

RECTIFICATIF TECHNIQUE 3

Technical Corrigendum 3 to ISO/IEC 9798-2:2008 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*. Corrigendum 3 cancels and replaces ISO/IEC 9798-2:2008/Cor.1:2010 and ISO/IEC 9798-2:2008/Cor.2:2012.

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.3:2013(E)**

Published in Switzerland

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.

— 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.

h) In the mechanisms specified in Clause 7, the holder of a key K_{AP} (or K_{BP}) shall always use it in the same way, i.e. acting either as the TTP *P* or as the entity *A* (or *B*). That is, no entity shall act as the TTP in one instance of a protocol and act as *A* or *B* in another instance of the protocol, and use the same key in both cases.

Page 16, Bibliography

Add the following reference to the Bibliography:

[1] D. Basin, C. Cremers and S. Meier, 'Provably repairing the ISO/IEC 9798 standard for entity authentication'. In: P. Degano, J. D. Guttman (eds.), *Principles of Security and Trust - First International Conference, POST 2012, Tallinn, Estonia, March 24 – April 1, 2012, Proceedings*. Springer LNCS 7215, pp.129-148, 2012.

