**INTERNATIONAL STANDARD ISO/IEC 9798-3:1998**
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 3:
## Mechanisms using digital signature techniques

TECHNICAL CORRIGENDUM 2

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

*Partie 3: Mécanismes utilisant des techniques de signature numériques*

*RECTIFICATIF TECHNIQUE 2*

Technical Corrigendum 2 to ISO/IEC 9798-3:1998 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

---

*Page 1, Clause 4*

Replace the following text:

If either of these is not satisfied then the authentication process may be compromised or it cannot be completed successfully.

NOTES

1 One way of obtaining a valid public key is by means of a certificate (see Annex C of ISO/IEC 9798-1). The generation, distribution, and revocation of certificates are outside the scope of this part of ISO/IEC 9798. There may exist a trusted third party for this purpose. Another way of obtaining a valid public key is by trusted courier.

2 References to digital signature schemes are contained in Annex D of ISO/IEC 9798-1.

**ICS 35.040** **Ref. No. ISO/IEC 9798-3:1998/Cor.2:2012(E)**



Published in Switzerland

with:

c) The private signature key used in an implementation of one of the mechanisms specified in this part of ISO/IEC 9798 shall be distinct from keys used for any other purposes.

d) The data strings signed 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 signed data string:

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

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

The recipient of a signature shall verify that the object identifier and the constant identifying the signature position within the mechanism are as expected.

If any of these is not satisfied then the authentication process may be compromised or it cannot be completed successfully.

NOTE 1 One way of obtaining a valid public key is by means of a certificate (see Annex C of ISO/IEC 9798-1). The generation, distribution, and revocation of certificates are outside the scope of this part of ISO/IEC 9798. There may exist a trusted third party for this purpose. Another way of obtaining a valid public key is by trusted courier.

NOTE 2 References to digital signature schemes are contained in the Bibliography of ISO/IEC 9798-3:1998/Amd.1:2010.