Information technology — Security techniques — Entity authentication —

Part 4:
Mechanisms using a cryptographic check function

TECHNICAL CORRIGENDUM 2

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

Partie 4: Mécanismes utilisant une fonction cryptographique de vérification

RECTIFICATIF TECHNIQUE 2

Technical Corrigendum 2 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 iv, Foreword

Add the following text at the end of Foreword:

Annex B of this part of ISO/IEC 9798 is normative, and defines object identifiers.

ICS 35.040

Ref. No. ISO/IEC 9798-4:1999/Cor.2:2012(E)

Page 2, Clause 4

Add the following text at the end of Clause 4:

d) The secret authentication key used in implementations of any of the mechanisms specified in this part of ISO/IEC 9798 shall be distinct from the keys used for any other purposes.

e) The cryptographic check values used at various places in an authentication mechanism shall not be interchangeable.

> NOTE   This could be enforced by including the following elements in the data string used to compute each cryptographic check value:
>
> — 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 cryptographic check value within the mechanism. This constant may be omitted in mechanisms that include only one cryptographic check value.

The recipient of a cryptographic check value shall verify that the object identifier and the constant identifying the cryptographic check value are as expected.

Page 7, Annex A

Add the following Annex B after the end of Annex A:

Annex B
(normative)

Object Identifiers

This annex lists the object identifiers assigned to mechanisms specified in this part of ISO/IEC 9798.

```
EntityAuthenticationMechanisms-4   {iso(1)   standard(0)   e-auth-mechanisms(9798)
                                   part4(4) asn1-module(0) object-identifiers(0)}

DEFINITIONS EXPLICIT TAGS ::= BEGIN

-- EXPORTS All; --

-- IMPORTS None; --

OID ::= OBJECT IDENTIFIER -- alias

-- Synonyms --

is9798-4 OID ::= {iso(1) standard(0) e-auth-mechanisms(9798) part4(4)}

mechanism OID ::= {is9798-4 mechanisms(1)}

-- unilateral authentication mechanisms --

ua-one-pass OID ::= {mechanism ua-One-pass(1)}
```