INTERNATIONAL STANDARD ISO/IEC 11770-4:2006
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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 11770-4:2006/Cor 1:2009

Information technology — Security techniques — Key management —

Part 4: Mechanisms based on weak secrets

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Techniques de sécurité — Gestion de clés —

Partie 4: Mécanismes basés sur des secrets faibles

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 11770-4:2006 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page 7, Clause 4

Replace the definition of || with the following:

> *X* ||*Y* denotes the result of the concatenation of octet strings *X* and *Y* in the order specified. In cases where the result of concatenating two or more octet strings is input to a cryptographic function as part of one of the mechanisms specified in this part of ISO/IEC 11770, this result shall be composed so that it can be uniquely resolved into its constituent octet 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 octet strings throughout the domain of use of the mechanism, or (b) encoding the sequence of concatenated octet strings using a method that guarantees unique decoding, e.g. using the distinguished encoding rules defined in ISO/IEC 8825-1 [ISO/IEC 8825-1].

ICS 35.040 **Ref. No. ISO/IEC 11770-4:2006/Cor.1:2009(E)**

© ISO/IEC 2009 – All rights reserved

Published in Switzerland