INTERNATIONAL STANDARD ISO/IEC11770-3:2015
TECHNICAL CORRIGENDUM 1

Published 2016-05-15

Information technology — Security techniques — Key management —

Part 3: Mechanisms using asymmetric techniques

TECHNICAL CORRIGENDUM 1

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

Partie 3: Mécanismes utilisant des techniques asymétriques

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 11770-3:2015 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques.*

Page 6, Clause 3 Terms and definitions

Add the following after 3.43 and renumber all the terms and definitions alphabetically:

3.44
resilience to key compromise impersonation attack on A
resilience to attacks in which an adversary exploits knowledge of the long-term private key of A to impersonate any entity in subsequent communication with A

3.45
resilience to unknown key share attack for A and B
resilience to attacks in which only A and B know the session key K; however, A and B disagree on who they share K with

ICS 35.040 **Ref. No. ISO/IEC 11770-3:2015/Cor.1:2016(E)**

Note 1 to entry: Resilience to unknown key share attack can be achieved by choosing a key derivation function that includes the identifiers of the involved entities.

Page 15, 11.1 Key agreement mechanism 1

Add the following after NOTE 5:

NOTE 6 This mechanism is not resilient to key compromise impersonation attack on A.

Page 18, 11.3 Key agreement mechanism 3

Add the following after NOTE 7:

NOTE 8 This mechanism is not resilient to key compromise impersonation attack on A.

Page 21, 11.6 Key agreement mechanism 6

Add the following after NOTE 8:

NOTE 9 This mechanism is not resilient to key compromise impersonation attack on A.

Page 23, 11.8 Key agreement mechanism 8

Add the following after NOTE 3:

NOTE 4 This mechanism is not resilient to key compromise impersonation attack on A.