



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