INTERNATIONAL STANDARD ISO/IEC 19790:2006
TECHNICAL CORRIGENDUM 1

Published 2008-06-15

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 — Security requirements for cryptographic modules

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Techniques de sécurité — Exigences de sécurité pour les modules cryptographiques

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 19790:2006 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page 34

Add the following subclause before 7.9:

7.8.2.5 Software/firmware load test

If software or firmware components can be externally loaded into a cryptographic module, then the following software/firmware load tests shall be performed:

1. Application of an Approved authentication technique (e.g. an Approved message authentication code, digital signature algorithm, or HMAC) to all validated software and firmware components when the components are externally loaded into a cryptographic module. The software/firmware load test is not required for any software and firmware components excluded from the security requirements of this International Standard (refer to clause 7.1).

2. Comparison of the calculated result with a previously generated result. If the calculated result does not equal the previously generated result, the software/firmware load test fails.

ICS 35.040 **Ref. No. ISO/IEC 19790:2006/Cor.1:2008(E)**

Published in Switzerland