
**Information technology — Security
techniques — Key management —**

Part 4:

Mechanisms based on weak secrets

**AMENDMENT 1: Unbalanced Password-
Authenticated Key Agreement with
Identity-Based Cryptosystems (UPAKA-
IBC)**

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

Partie 4: Mécanismes basés sur des secrets faibles

*AMENDEMENT 1: Accord dissymétrique de clé authentifié par mot de
passe utilisant un mécanisme de chiffrement basé sur l'identité*



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland