INTERNATIONAL STANDARD

ISO/IEC 29180

First edition
2012-12-01

Information technology — Telecommunications and information exchange between systems — Security framework for ubiquitous sensor networks

Technologies de l'information — Télécommunications et échange d'informations entre systèmes — Cadre de sécurité pour réseaux de capteurs ubiquitaires

Reference number
ISO/IEC 29180:2012(E)

© ISO/IEC 2012

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

CONTENTS

© ISO/IEC 2012 – All rights reserved

 © ISO/IEC 2012 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29180 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*, in collaboration with ITU-T. The identical text is published as Rec. ITU-T X.1311 (02/2011).

© ISO/IEC 2012 – All rights reserved

Introduction

This Recommendation | International Standard describes the security threats to and security requirements of the ubiquitous sensor network. In addition, this Recommendation | International Standard categorizes the security technologies according to the security functions that satisfy the said security requirements and where the security technologies are applied in the security model of ubiquitous sensor networks. Finally, the security functional requirements and security technologies for the ubiquitous sensor networks are presented.

© ISO/IEC 2012 – All rights reserved

INTERNATIONAL STANDARD
RECOMMENDATION ITU-T

Information technology – Security framework for ubiquitous sensor networks

1 Scope

The recent advancement of wireless-based communication technology and electronics has facilitated the implementation of a low-cost, low-power sensor network. Basically, a ubiquitous sensor network (USN) consists of three parts: a sensor network consisting of a large number of sensor nodes, a base station (also known as a gateway) interfacing between the sensor networks and an application server, and the application server controlling the sensor node in the sensor network or collecting the sensed information from the sensor nodes in the sensor network.

USN can be an intelligent information infrastructure of advanced e-Life society, which delivers user-oriented information and provides knowledge services to anyone anytime, anywhere and wherein information and knowledge are developed using context awareness by detecting, storing, processing, and integrating the situational and environmental information gathered from sensor tags and/or sensor nodes affixed to anything. Since there are many security and privacy threats in transferring and storing information in the USN, appropriate security mechanisms may be needed to protect against those threats in the USN.

This Recommendation | International Standard describes the security threats to and security requirements of the ubiquitous sensor network. In addition, this Recommendation | International Standard categorizes the security technologies according to the security functions that satisfy the said security requirements and where the security technologies are applied in the security model of the USN. Finally, the security requirements and security technologies for the USN are presented.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

None.

2.2 Paired Recommendations | International Standards equivalent in technical content

– Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

ISO/IEC 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

– Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

ISO/IEC 18028-2:2006, *Information technology – Security techniques – IT network security – Part 2: Network security architecture*.

2.3 Additional references

– Recommendation ITU-T H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.

– Recommendation ITU-T X.1111 (2007), *Framework of security technologies for home network*.

– Recommendation ITU-T X.1191 (2009), *Functional requirements and architecture for IPTV security aspects*.

– Recommendation ITU-T Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment*.

– Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

– FIPS PUB 140-2 (2001), *Security Requirements for Cryptographic Modules*.