ISO/IEC 29180:2012-12 (E)

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

Contents

Page

Reference number INTERNATIONAL STANDARD 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 COPYRIGHT PROTECTED DOCUMENT 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 1 Scope 1

2 Normative references 1
2.1 Identical Recommendations ..... International Standards| 1
2.2 Paired Recommendations ..... International Standards equivalent in technical content| 1
2.3 Additional references 1

3 Definitions 2
3.1 Terms defined elsewhere 2
3.2 Terms defined in this Recommendation ..... International Standard| 2

4 Abbreviations 3

5 Conventions 4

6 Overview 4

7 Threats and security models for ubiquitous sensor networks 7
7.1 Threat models in sensor networks 7
7.2 Threat models in IP networks 10
7.3 Security model for USNs 10

8 General security dimensions for USN 10

9 Security dimensions and threats in ubiquitous sensor networks 11
9.1 Security dimensions and threats for the message exchange in sensor networks 11
9.2 Security dimension and threats for the message exchange in the IP network 14

10 Security techniques for ubiquitous sensor networks 14
10.1 Key management 14
10.2 Authenticated broadcast 15
10.3 Secure data aggregation 16
10.4 Data freshness 17
10.5 Tamper-resistant module 17
10.6 USN middleware security 17
10.7 IP network security 17
10.8 Sensor node authentication 18
10.9 Privacy protection in sensor networks 18

11 Specific security functional requirements for USN 18
11.1 Mandatory functional requirement 18
11.2 Recommended functional specifications 18

11.3 Optional functional specifications 18

Annex A - Key management in sensor networks 20

A.1 Threat time 20
A.2 Key management classes 20
A.3 Key schemes 21

Annex B - Authenticated broadcast in sensor networks: µTPC 23

B.1 Construction of µTPC 23
B.2 Construction of µTPCT 24
B.3 Authenticated broadcast 25

Annex C - Authentication mechanisms in sensor networks 26

C.1 XOR-based mechanism 26
C.2 Hash-based mechanism 27
C.3 Public key-based authentication 29

Annex D - Secure data aggregation in sensor networks 32

D.1 Elect aggregation node and supervisor 32
D.2 Implementation of supervisor functions 33
D.3 Upload supervising message 33
D.4 Determine the trust of aggregation nodes 33
D.5 Send revocation message 33

Bibliography 34