INTERNATIONAL STANDARD

ISO/IEC 21277

First edition
2018-02

Information technology — Radio frequency identification device performance test methods — Crypto suite

Technologies de l'information — Méthodes de test de performance des systèmes d'identification par radiofréquence (RFID) — Suites cryptographiques

Reference number
ISO/IEC 21277:2018(E)

© ISO/IEC 2018



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

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, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **2**
5 Measurement context ... **2**
6 Setup of test equipment ... **2**
7 System parameters ... **3**
7.1 General ... 3
7.2 Crypto performance ... 3
7.3 Interrogator-system architecture ... 3
8 Measurements in scope ... **3**
9 Test method ... **4**
Annex A (informative) **Interrogator crypto suite implementation** ... **7**
Annex B (informative) **Security suite application considerations** ... **8**
Bibliography ... **9**

© ISO/IEC 2018 – 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

© ISO/IEC 2018 – All rights reserved

Introduction

ISO/IEC 18000 defines the air interfaces for radio frequency identification (RFID) devices used in item management applications. ISO/IEC 18000-63 defines the air interface for these devices operating at frequencies from 860 MHz to 960 MHz Type C.

ISO/IEC 29167 defines crypto suite air interfaces for ISO/IEC 18000-63 utilising on tag cryptography functions.

This document provides test methods for performance measurement of the ISO/IEC 29167 devices.

NOTE This specification is a system measurement of tag and interrogator performance.

© ISO/IEC 2018 – All rights reserved

Information technology — Radio frequency identification device performance test methods — Crypto suite

1 Scope

This document defines test methods to measure the performance of crypto suites of radio frequency identification (RFID) devices (tags and interrogators) for item management as specified in ISO/IEC 18000-63 and ISO/IEC 29167 (all parts).

These test methods measure the crypto suite system performance (tags and interrogators) against the crypto suite outcomes as required by the desired set of use case requirements for a specific application/service. These test methods are used as an extension of ISO/IEC 18046-1 but can be used in a standalone manner.

Crypto suite performance can vary substantially between crypto suites, implementations of a crypto suite for tags and interrogators and crypto suite outcomes in specific interrogation scenarios. Tag crypto functions require time and energy to complete successfully. The desired crypto strength and method influence the time and energy required. "Crypto suite performance" is therefore defined in this document as "the shortest time to complete a crypto outcome at a given read distance in relation to the RF power available". This document provides guidelines in the evaluation of the measurement results.

The test methods do not measure crypto capabilities which include crypto strength, suitability and robustness. They neither measure random generator performance nor deal with key management.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18000-63, *Information technology — Radio frequency identification for item management — Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C*

ISO/IEC 18046-1, *Information technology — Radio frequency identification device performance test methods — Part 1: Test methods for system performance*

ISO/IEC 19762, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 and ISO/IEC 18000-63 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

© ISO/IEC 2018 – All rights reserved