FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEEE
FDIS
18880-3**

ISO/TC **215**

Secretariat: **ANSI**

ISO voting begins on:
2015-10-01

ISO voting terminates on:
2016-03-01

Information technology — Ubiquitous green community control network —

Part 3:
Security

Titre manque —

Partie 3: ???

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION. SEE ADDITIONAL INFORMATION ABOUT PATENTS ON THE INSIDE BACK COVER. BECAUSE IT IS AN UNAPPROVED DRAFT, THIS DOCUMENT SHALL NOT BE USED FOR ANY CONFORMANCE/COMPLIANCE PURPOSES.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

**Please see the administrative notes on page iii
and on the inside back cover**

Reference number
ISO/IEEE FDIS 18880-3:2015(E)

© ISO 2015
© IEEE 2015

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. Neither the ISO Central Secretariat nor IEEE accepts any liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies and IEEE members. In the unlikely event that a problem relating to it is found, please inform the ISO Central Secretariat or IEEE at the address given below.

Copyright notice

This ISO/IEEE document is a Final Draft International Standard and is copyright-protected by ISO and IEEE. Except as permitted under the applicable laws of the user's country, neither this ISO/IEEE draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester. In the United States, such requests should be sent to IEEE.

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

Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York • NY 10016-5997, USA
E-mail stds.ipr@ieee.org
Web www.ieee.org

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

© ISO 2015 – All rights reserved
© IEEE 2015 – All rights reserved

FAST-TRACK PROCEDURE

This document is submitted under the fast-track procedure in accordance with the Partner Standards Development Organization cooperation agreement between ISO and IEEE, as approved by Council Resolution 49/2007, and is submitted to all ISO member bodies for voting within 5 months.

Positive votes shall not be accompanied by comments.

Negative votes shall be accompanied by the relevant technical reasons.

In accordance with the provisions of Council Resolution 15/1993, this document is **circulated in the English language only**.

© ISO 2015 – All rights reserved
© IEEE 2015 – 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.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

The main task of ISO/IEC JTC 1 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 called to the possibility that implementation of this standard may require the use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. ISO/IEEE is not responsible for identifying essential patents or patent claims for which a license may be required, for conducting inquiries into the legal validity or scope of patents or patent claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance or a Patent Statement and Licensing Declaration Form, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from ISO or the IEEE Standards Association.

ISO/IEC/IEEE 18880-3 was prepared by the Corporate Advisory Group of the IEEE-SA Board of Governors (as IEEE 1888.3-2013). It was adopted by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems,* in parallel with its approval by the ISO/IEC national bodies, under the “fast-track procedure” defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE. IEEE is responsible for the maintenance of this document with participation and input from ISO/IEC national bodies.

© ISO 2015 – All rights reserved

© IEEE 2015 – All rights reserved

IEEE STANDARDS ASSOCIATION

IEEE Standard for Ubiquitous Green Community Control Network: Security

IEEE-SA Board of Governors

Sponsored by the
Corporate Advisory Group

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 1888.3™-2013

IEEE Standard for Ubiquitous Green Community Control Network: Security

Sponsor

Corporate Advisory Group
of the
IEEE-SA Board of Governors

Approved 31 October 2013

IEEE-SA Standards Board

© ISO 2015 – All rights reserved
© IEEE 2015 – All rights reserved

Abstract: The enhanced security management function for the protocol defined in IEEE 1888™, "Ubiquitous Green Community Control Network Protocol," is described in this standard. Security requirements, system security architecture definitions, and a standardized description of authentication and authorization, along with security procedures and protocols, are specified. This standard can help avoid unintended data disclosure to the public and unauthorized access to resources, while providing enhanced integrity and confidentiality of transmitted data in the ubiquitous green community control network.

Keywords: access control, authorization, certificate, confidentiality, IEEE 1888™, IEEE 1888.3™, integrity, mutual authentication, security

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2013 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 6 December 2013. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-7381-8725-9 STD98436
Print: ISBN 978-0-7381-8726-6 STDPD98436

IEEE prohibits discrimination, harassment, and bullying.
For more information, visit http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

© ISO 2015 – All rights reserved
© IEEE 2015 – All rights reserved

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association ("IEEE-SA") Standards Board. IEEE ("the Institute") develops its standards through a consensus development process, approved by the American National Standards Institute ("ANSI"), which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

© ISO 2015 – All rights reserved
© IEEE 2015 – All rights reserved

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

© ISO 2015 – All rights reserved
© IEEE 2015 – All rights reserved

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at http://ieeexplore.ieee.org/xpl/standards.jsp or contact IEEE at the address listed previously. For more information about the IEEE-SA or IEEE's standards development process, visit the IEEE-SA Website at http://standards.ieee.org.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: http://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at http://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

© ISO 2015 – All rights reserved
© IEEE 2015 – All rights reserved

Participants

At the time this IEEE standard was completed, the UGCCNet-SEC Working Group had the following membership:

Dong Liu, *Chair*
Wenjie Li, *Vice Chair*

Beijing Jiaotong University
BII Group Holdings Ltd.
China Telecommunications Corporation
Cisco Systems Inc.
Intel Corporation
Qingdao Gaoxiao Information Industry Co., Ltd.
Raisecom Technology Co., Ltd
The University of Tokyo

The P1888.3 Working Group gratefully acknowledges the contributions of the following participants. Without their assistance and dedication, this standard would not have been completed.

Changhe Du
Chen Gu
Dong Liu
Guoquan Tan
Hideya Ochiai
Hiroshi Esaki
Hongke Zhang
Huiling Zhao
Lianshan Jiang
Masahiro Ishiyama
Ming Feng
Ming Qiu
Ning Zou
Shoichi Sakane
Shuai Gao
Tsuyoshi Momose
Wenjie Li
Wenjie Ma
Xiaochuan Gu
Yan He

The following members of the entity balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Beijing Jiaotong University
BII Group Holdings Ltd.
China Datang Corporation
China Telecommunications Corporation
Cisco Systems, Inc.
Intel Corporation
Marvell Semiconductor, Inc.
Nippon Telegraph and Telephone Corporation (NTT)
NXP Semiconductors
Qingdao Gaoxiao Information Industry Co. Ltd.
Raisecom Technology Co., Ltd.
The University of Tokyo

When the IEEE-SA Standards Board approved this standard on 31 October 2013, it had the following membership:

John Kulick, *Chair*
David J. Law, *Vice Chair*
Richard H. Hulett, *Past Chair*
Konstantinos Karachalios, *Secretary*

Masayuki Ariyoshi
Peter Balma
Farooq Bari
Ted Burse
Wael William Diab
Stephen Dukes
Jean-Philippe Faure
Alexander Gelman
Mark Halpin
Gary Hoffman
Paul Houzé
Jim Hughes
Michael Janezic
Joseph L. Koepfinger*
Oleg Logvinov
Ron Petersen
Gary Robinson
Jon Walter Rosdahl
Adrian Stephens
Peter Sutherland
Yatin Trivedi
Phil Winston
Yu Yuan

*Member Emeritus

Copyright © 2013 IEEE. All rights reserved.
© ISO 2015 – All rights reserved
© IEEE 2015 – All rights reserved

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Richard DeBlasio, *DOE Representative*
Michael Janezic, *NIST Representative*

Patrick Gibbons
IEEE Standards Program Manager, Document Development

Krista Gluchoski
IEEE Project Specialist, Professional Services

Joan Woolery
IEEE Standards Program Manager, Technical Program Development

Copyright © 2013 IEEE. All rights reserved.

© ISO 2015 – All rights reserved
© IEEE 2015 – All rights reserved

Introduction

This introduction is not part of IEEE Std 1888.3-2013, IEEE Standard for Ubiquitous Green Community Control Network: Security.

This standard describes the enhanced security management function for the protocol defined in IEEE Std 1888™, IEEE Standard for Ubiquitous Green Community Control Network Protocol, specifies security requirements, defines system security architecture, gives a standardized description of authentication and authorization, along with security procedures and protocols. This standard can help avoid unintended data disclosure to the public and unauthorized access to resources, while providing enhanced integrity and confidentiality of transmitted data in the ubiquitous green community control network.

The purpose of this standard is to define a security management function in the ubiquitous green community control network that provides an interoperable, high-quality, and secure applications operation platform. As an open system, a ubiquitous green community control network assumes multi-domain operation and public access from other system components. In this context, security considerations are needed for operation of the IEEE 1888 protocol.

This specification defines the architecture and framework that provides security for IEEE 1888 systems. As an interactive monitoring and control system based on sensor-actuator networks, IEEE 1888 systems without security suffer from some potential security threats. For example, unintended users or systems may capture sensor readings and control HVAC or lights easily, or information exchanged and data stored may be overwritten by unauthorized users or components. This standard specifies a security framework to protect the message exchange path of both the data plane and the control plane of an IEEE 1888 system from such security threats, providing mutual authentication, access control, message integrity, data confidentiality, and so on.

The IEEE 1888 protocol is bound to simple object access protocol (SOAP) and normally takes hypertext transfer protocol (HTTP) for the transportation of its SOAP messages. To meet the security requirements and protect from security threats, HTTP over TLS (HTTPS) shall be adopted. This is because HTTPS has been widely used and can satisfy the security requirements with small implementation cost.

This document distinguishes system reliability issues from security issues. For example, service tolerance against heavy requests from clients and communication tolerance against temporal physical link failure are out of the scope of this document.

This document is organized as follows:

- Clause 4 specifies security requirements and design principles.
- Clause 5 describes security system architecture.
- Clause 6 defines security protocols, including communication sequence, software interface, and identifier (ID) system.

Copyright © 2013 IEEE. All rights reserved.

© ISO 2015 – All rights reserved
© IEEE 2015 – All rights reserved

Contents

1. Overview 1
1.1 Scope 1
1.2 Purpose 1

2. References 2
2.1 Normative references 2
2.2 Additional References 2

3. Definitions, abbreviations, and acronyms 3
3.1 Definitions 3
3.2 Abbreviations and acronyms 3

4. Security requirements and design principles 4
4.1 Security issues overview 4
4.2 Security requirements 6
4.3 Design principles 7

5. Security architecture 8
5.1 System architecture 8
5.2 Initiator and responder 9
5.3 Identifier 9

6. Security protocols 10
6.1 Communication sequence 10
6.2 Interface definition 11
6.3 Authentication, Authorization, and Accounting (AAA) Function definition 14
6.4 Rejecting connection 18

Copyright © 2013 IEEE. All rights reserved.

© ISO 2015 – All rights reserved
© IEEE 2015 – All rights reserved

IEEE Standard for Ubiquitous Green Community Control Network: Security

IMPORTANT NOTICE: IEEE Standards documents are not intended to ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

1. Overview

1.1 Scope

This specification provides security service enhancements for the protocol defined in IEEE Std 1888™[1], IEEE Standard for Ubiquitous Green Community Control Network Protocol. This standard describes security requirements for the ubiquitous green community control network and specifies the system security architecture along with security procedures and protocols.

1.2 Purpose

The purpose of this standard is to define a security management function in the ubiquitous green community control network that provides an interoperable, high-quality, and secure applications operation platform. Use of this standard helps avoid unintended data disclosure to the public and unauthorized access to resources, while providing enhanced integrity and confidentiality of transmitted data in the ubiquitous green community control network.

[1] Information on references can be found in Clause 2.

Copyright © 2013 IEEE. All rights reserved.

© ISO 2015 – All rights reserved
© IEEE 2015 – All rights reserved

2. References

2.1 Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 1888™, IEEE Standard for Ubiquitous Green Community Control Network Protocol.[2, 3]

RFC 791, Internet Protocol, J. Postel, Ed., September 1981.[4]

RFC 1035, Domain Names—Implementation and Specification, P. Mockapetris, November 1987.

RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, R. Housley, W. Ford, W. Polk, and D. Solo, January 1999.

RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, S. Deering and R. Hinden, December 1998.

RFC 5246, The Transport Layer Security (TLS) Protocol, Version 1.2, T. Dierks and E. Rescorla, August 2008.

RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, May 2008.

RFC 5322, Internet Message Format, P. Resnick, Ed., October 2008.

RFC 6066, Transport Layer Security (TLS) Extensions: Extension Definitions, D. Eastlake, III, January 2011.

2.2 Additional references

RFC 6277, “Online Certificate Status Protocol Algorithm Agility,” S. Santesson and P. Hallam-Baker, June 2011.

The OpenSSL Project website.[5]

[2] The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.
[3] IEEE publications are available from The Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).
[4] IETF documents (i.e. RFCs) are available for download at http://www.rfc-archive.org/.
[5] Available at: http://www.openssl.org/

Copyright © 2013 IEEE. All rights reserved.

© ISO 2015 – All rights reserved
© IEEE 2015 – All rights reserved

3. Definitions, abbreviations, and acronyms

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause. [6]

access control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

binding information: The association of the identifier (ID) of a client-role certificate of the responder with an access uniform resource identifier (URI) for the responder along with the remaining lifetime of that association.

confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

data integrity: The property that data has not been altered or destroyed in an unauthorized manner without detection or awareness.

digital signature: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to verify the source and integrity of the data unit and protect against forgery.

3.2 Abbreviations and acronyms

AAA	authentication, authorization, and accounting
ACL	access control list
ACM	access control manager
AM	authentication manager
APP	application
CA	certificate authority
CV	certificate verification
DNS	domain-name system
DoS	denial of service
DDoS	distributed denial of service
FQDN	fully qualified domain name
GW	gateway

[6] *IEEE Standards Dictionary Online* subscription is available at: http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html.

Copyright © 2013 IEEE. All rights reserved.

© ISO 2015 – All rights reserved
© IEEE 2015 – All rights reserved