IEEE STANDARDS ASSOCIATION

IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP)

IEEE Computer Society

Sponsored by the
Design Automation Standards Committee

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

IEEE Std 1735™-2014
(Incorporates
IEEE Std 1735-2014/Cor 1-2015)

IEEE Std 1735™-2014
(Incorporates
IEEE Std 1735-2014/Cor 1-2015)

IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP)

Sponsor

Design Automation Standards Committee
of the
IEEE Computer Society

Approved 10 December 2014

IEEE SA-Standards Board

Acknowledgments

Grateful acknowledgment is made to the following for the permission to use the following source material:

Accellera/VSIA—*IP_Encrypt_VSIAtoIEEE.doc*: VSIA contribution from the IP-Encrypt Working Group.

Cadence—Material in clause titled “Rights Management” is derived from the document titled “Rights Management Specification for Verilog® Protected Envelopes” © 2007, 2011, Cadence Design Systems Inc. Used, modified, and reprinted by permission of Cadence Design Systems Inc.

Synopsys—*IP_Licensing_Recommendations_for_P1735.pptx*: Synopsys IP licensing overview.

Abstract: Guidance on technical protection measures to those who produce, use, process, or standardize the specifications of electronic design intellectual property (IP) are provided in this recommended practice. Distribution of IP creates a risk of unsanctioned use and dilution of the investment in its creation. The measures presented here include protection through encryption, specification, and management of use rights that have been granted by the producers of electronic designs, and methods for integrating license verification for granted rights.

Keywords: digital envelope, encrypted IP, IEEE 1735™, keys, rights management, trust model

---

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

Print: ISBN 978-0-7381-9492-9 STD20084
PDF: ISBN 978-0-7381-9493-6 STDPD20084

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.

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.

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/expel/standards.jsp or contact IEEE at the address listed previously. For more information about the IEEE-SA or IOWA'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.

Participants

IEEE Std 1735-2014

The Electronic Design Intellectual Property (IP) Working Group is entity based. At the time this standard was completed, the Electronic Design Intellectual Property (IP) Working Group had the following membership:

Dave Graubart, *Chair*
Joe Daniels, *Technical Editor*

Luis Humberto Rezende Barbosa
Dave Clemans
Steven Dovich
Jeff Fox
Parminder Gill
Satyam Jani
Jarek Kaczynski
Ray Martin
Gael Paul
Rod Price
Adam Sherer
John Shields
Michael Smith
Sourabh Tandon
Ruchi Tyagi

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

Accellera Organization, Inc.
ALDEC, Inc.
Altera Corporation
Atrenta Inc.
Cadence Design Systems, Inc.
Mentor Graphics
Synopsys, Inc.
Xilinx Inc.

When the IEEE-SA Standards Board approved this standard on 10 December 2014, it had the following membership:

John Kulick, *Chair*
Jon Walter Rosdahl, *Vice Chair*
Richard H. Hulett, *Past Chair*
Konstantinos Karachalios, *Secretary*

Peter Balma
Farooq Bari
Ted Burse
Clint Chaplain
Stephen Dukes
Jean-Phillippe Faure
Gary Hoffman
Michael Janezic
Jeffrey Katz
Joseph L. Koepfinger*
David J. Law
Hung Ling
Oleg Logvinov
T. W. Olsen
Glenn Parsons
Ron Peterson
Adrian Stephens
Peter Sutherland
Yatin Trivedi
Phil Winston
Don Wright
Yu Yuan

*Member Emeritus

At the time this standard was completed, the Electronic Design Intellectual Property (IP) Working Group had the following membership:

Dave Graubart, *Chair*
Joe Daniels, *Technical Editor*

Luis Humberto Rezende Barbosa
Dave Clemans
Steven Dovich
Jeff Fox
Parminder Gill
Satyam Jani
Jarek Kaczynski
Ray Martin
Gael Paul
Rod Price
Adam Sherer
John Shields
Michael Smith
Sourabh Tandon
Ruchi Tyagi

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

Accellera Organization, Inc.
ALDEC, Inc.
Altera Corporation
Atrenta Inc.
Cadence Design Systems, Inc.
Marvell Semiconductor, Inc.
Mentor Graphics
Micron Technology, Inc.
Synopsys, Inc.
Xilinx Inc.

When the IEEE-SA Standards Board approved this standard on 3 September 2015, it had the following membership:

John D. Kulick, *Chair*
Jon Walter Rosdahl, *Vice Chair*
Richard H. Hulett, *Past Chair*
Konstantinos Karachalios, *Secretary*

Masayuki Ariyoshi
Ted Burse
Stephen Dukes
Jean-Philippe Faure
J. Travis Griffith
Gary Hoffman
Michael Janezic
Joseph L. Koepfinger*
David J. Law
Hung Ling
Andrew Myles
T. W. Olsen
Glenn Parsons
Ronald C. Petersen
Annette D. Reilly
Stephen J. Shellhammer
Adrian P. Stephens
Yatin Trivedi
Phillip Winston
Don Wright
Yu Yuan
Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 1735™-2014, IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP).

The purpose of this recommended practice is to provide guidance on protection of *electronic design intellectual property* (IP). The audience for this standard includes IP producers, IP consumers, vendors of tools that process protected IP, and standards development groups for IP specification formats.

When the electronic design automation (EDA) industry began creating standards for use in specifying, simulating, and implementing electronic circuits, there was no active market for the exchange of electronic designs. As interest in software reuse developed, the EDA industry began to share design collateral as a means of controlling the cost of development and managing the timeline for completing their design projects. Because that shared IP had a measurable development cost, business leaders began to insist on recovering those costs through licensing to other potential uses. Technical measures for IP protection were developed to augment the legal contracts that governed such shared use.

As the means for technical protection of IP proliferated, there was increased pressure to incorporate that technology in the existing standards for representation of IP. Expertise in protection technologies (such as encryption) was scarce in those standards development organizations (SDOs), which resulted in a slow pace of development within a given standard and technical divergence as independent organizations attempted to solve similar problems. As the marketplace for IP exchange continued to mature, concerns about technical protection of IP extended to include an interest in defining and managing the scope of use for protected IP.

This standard has been created to consolidate EDA industry efforts to unify the technical protections for IP and to guide SDOs in aligning their work for interoperability and compatibility. It is also intended to share best practices in IP protection for those who use standards that incorporate such technology, such as VHDL (IEC 61691-1-1, IEEE Std 1076™) and SystemVerilog (IEEE Std 1800™).[a]

Corrections were made to 7.4.3 as required by IEEE Std 1735-2014/Cor 1-2015.

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

Contents

1. Overview 1

1.1 Scope 1
1.2 Purpose, value, and approach 2
1.3 Key characteristics of this standard 2
1.4 Conventions used in this standard 3
1.5 Use of color in this standard 3
1.6 Contents of this standard 4

2. Normative references 5

3. Definitions, acronyms, and abbreviations 5

3.1 Definitions 5
3.2 Acronyms and abbreviations 7

4. Trust model 8

4.1 Stakeholders 8
4.2 Role of IP protection 8
4.3 Protection via encryption 9
4.4 Components of trust 10

5. Interoperability 12

5.1 Background 12
5.2 version pragma 12
5.3 Basic interoperability 13
5.4 Use cases 16
5.5 Secure keyring 19

6. Key management 21

6.1 Overview 21
6.2 Key considerations 21
6.3 Basic key exchange 22
6.4 Standard key exchange 23
6.5 Key scope recommendations 25

7. Rights management [V2] 27

7.1 Introduction 27
7.2 Rights scope 27
7.3 Tool types and rights 27
7.4 Syntax and markup 28
7.5 Tamper-proof requirements 34
7.6 Complete tool block and rights example 34

8. License management [V2] 36

8.1 Introduction 36
8.2 License system 36
8.3 License proxy 36
8.4 License specification 36
8.5 License proxy parameters 37
8.6 License use 38
8.7 Multiple envelopes 39
8.8 Proxy communication 40
8.9 License proxy transactions 40
8.10 License proxy commands 44
8.11 Deprecated licensing pragmas 45

9. Visibility management 46

9.1 Introduction 46
9.2 Background [V1] 46
9.3 Visibility in tool phases [V1] 47
9.4 Visibility and encryption envelopes [V1] 50
9.5 **viewport** pragmas 52
9.6 Programming language interfaces 58
9.7 Controlling visibility with rights [V2] 60
9.8 Visibility of dynamic objects [V2] 61
9.9 Unresolved visibility issues 61

10. Common rights [V2] 62

10.1 Defining common rights 62
10.2 Overriding common rights 62
10.3 Defaults and the delegated value 62
10.4 Common conditions for rights 63
10.5 Common right for error handling 64
10.6 Common right for visibility 65
10.7 Common right for child visibility 66
10.8 Common right for decryption 67

Annex A (informative) Bibliography 68

Annex B (informative) Other known issues with IP protection 69

Annex C (normative) Protection pragmas 75

IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP)

1. Overview

1.1 Scope

This standard specifies embeddable and encapsulating markup syntaxes for design intellectual property encryption and rights management, together with recommendations for integration with design specification formats described in other standards. It also recommends use models for interoperable tool and hardware flows, which will include selecting encryption and encoding algorithms and encryption key management. The recommendation includes a description of the trust model assumed in the recommended use models. This standard does not specifically include any consideration of digitally encoded entertainment media. In the context of this document, the term *IP* will be used to mean *electronic design intellectual property*.

Electronic design intellectual property is a term used in the electronic design community. It refers to a reusable collection of design specifications that represent the behavior, properties, and/or representation of the design in various media. Examples of these collections include, but are not limited to, the following:

- A unit of electronic system design
- A design verification and analysis scheme (e.g., test bench)
- A netlist indicating elements and the interconnection thereof to implement a function
- A set of fabrication instructions
- A physical layout design or chip layout
- A design intent specification