
myProject™ - P1735 PAR Detail

Submitter Email: dovich@toolscribe.com

Type of Project: New IEEE Standard

PAR Request Date: 12-Oct-2007

PAR Approval Date: 27-Mar-2008

PAR Expiration Date: 31-Dec-2012

PAR Signature Page on File: No

Status: PAR for a New IEEE Standard

Project: 1735

Root Project:

1.1 Project Number: P1735

1.2 Type of Document: Recommended Practice

1.3 Life Cycle: Full Use

1.4 Is this project in ballot now? No

2.1 Title: Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP)

3.1 Working Group: Working Group for Design Intellectual Property (IP) Encryption and Rights Management (C/DA/C/DA/IP Encryption)

Contact Information for Working Group Chair

None

Contact Information for Working Group Vice-Chair

None

3.2 Sponsoring Society and Committee: IEEE Computer Society/Design Automation (C/DA)

Contact Information for Sponsor Chair

Victor Berman

Email: victorb@improvsys.com

Phone: 978 927 0555 x 27

Contact Information for Standards Representative

None

4.1 Type of Ballot: Entity

4.2 Expected Date of Submission for Initial Sponsor Ballot: 12/2009

4.3 Projected Completion Date for Submittal to RevCom: 06/2010

5.1 Approximate number of people expected to work on this project: 16

5.2 Scope: This standard specifies embeddable and encapsulating markup syntaxes for design IP 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 Intellectual Property electronic design data. Electronic Design Intellectual Property is

a term used in the electronic design community. It refers to a reusable collection of design specifications which represent the behavior, properties, and/or representation of the design in various media. Examples of these collections include, but are not limited to: · 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 The term is partially derived from the common practice for the collection to be considered the intellectual property of one party. Hardware and software descriptions are encompassed by this term.

5.3 Is the completion of this standard dependent upon the completion of another standard: No

5.4 Purpose: The purpose of this document is to enable design flows that provide interoperability between IP sources, tools, integrators, and users of the IP. There is currently no defined, independent standard for describing IP encryption markup for design information formats. Each design format which incorporates IP encryption describes their markup differently leading to confusing interpretation. Users of those standards also lack a recommended practice for inter-operable use of IP encryption. This document provides guidelines and recommended practice for use of IP protection markup syntax and key management to enable interoperable tool flows with IP and tools from a wide array of suppliers. It includes algorithm selection for encryption and encoding. This document specifies a generic set of embeddable markup syntax suitable for IP protection and rights management of arbitrary text files. These files represent potential inputs and outputs of EDA tools that would otherwise expose IP. The generic syntax of these directives may be suitably modified for a particular file format if there are syntactic conflicts and variations may be described in recommended practices.

5.5 Need for the Project: Working groups currently incorporating IP Encryption technologies use different descriptive language which makes shared implementation technology more difficult to produce, and the standards more difficult to interpret. Users of those standards also want further guidance on how to use the IP Encryption technologies for inter-operability.

5.6 Stakeholders for the Standard: Those that produce Design IP, including: digital system IP providers; those that use the IP provided: including systems integrators; and those that provide trusted hardware and/or software environments for working with the protected IP, including Field Programmable Gate Array providers, Silicon fabrication operations, and Electronic Design Automation Tool providers

Intellectual Property

6.1.a. Has the IEEE-SA policy on intellectual property been presented to those responsible for preparing/submitted this PAR prior to the PAR submittal to the IEEE-SA Standards Board? Yes

If yes, state date: 08/22/2007

6.1.b. Is the Sponsor aware of any copyright permissions needed for this project? Yes

If yes, please explain:Text from IEEE 1364-2005 and current draft of 1076 will be usefully incorporated. The VSI Alliance has sponsored a working group on this topic. That group has affirmed the willingness and capability to transfer copyright of their material, as individual members and as the corporation of VSI, to the P1735 project as asset and copyright transfers. The output of that working group is incomplete, but this statement has been made here to remove any concerns about material which might not yet be available.

6.1.c.Is the Sponsor aware of possible registration activity related to this project? No

7.1 Are there other standards or projects with a similar scope? Yes

If yes, please explain:IEEE Std 1364-2005 contains related specification, as does the current P1076 draft. The need for similar embedded markup exists for files which contain structured text and other languages for which standardization in other forums is desired. Where other forums are not active, it is hoped that a generic encapsulation recommendation can be written that will provide for language independent encapsulation. Questions on interpretation and intent arise in existing working groups and there is no clear consensus on which working group should take the lead in resolving these liaison issues. It is proposed that the DASC act as the unification forum for these topics, and that the P1735 be the focus group. There is significant activity in the rest of the standards world on encryption, it has been surveyed and no scope overlap has been identified. The closest activity is on XML encryption in the World Wide Web Consortium (W3C), and we have liaison activity initiated with that group. The scope of application between the W3C group and this proposed group differ significantly. IEEE 1619.3 is working on key management specifications. This will be a reference resource, but 1619.3 group is working in a different use context, one that includes movies and entertainment files. These are specifically excluded from the scope of P1735.

and answer the following:

Sponsor Organization: DASC

Project/Standard Number: P1800 & P1076

Project/Standard Date: 12/30/2008

Project/Standard Title: System Verilog & VHDL

7.2 Future Adoptions

Is there potential for this standard (in part or in whole) to be adopted by another national, regional, or international organization? Yes

If Yes, the following questions must be answered:

Other Organization Contact Information: IEC 93 3

Contact Person: general

Contact Phone:

Contact Email Address:

7.3 Will this project result in any health, safety, security, or environmental guidance that affects or applies to human health or safety? No

7.4 Additional Explanatory Notes: (Item Number and Explanation) 7.1 Other standards or projects with Similar Scope
Sponsor: DASC Project Number: P1076 Project Date: ballot pending Project Title: IEEE Standard VHDL Language Reference Manual