P1800 Requirements for IP Protection

John Shields

Two questions

- **What contribution will P1735 make that affects the P1800 LRM?**
- **What expectations does P1735 have of the P1800 WG?**

P1735 Charter

- **P1735 has been chartered by DASC to reconcile the IP Encryption and Design Protection technologies across the family of DASC sponsored standards. Our PAR specifies a "Recommended Practices" document, targeted at three communities:**
  - **IP producers looking for best practices guidance**
  - **EDA tool providers/users looking for inter-operability**
  - **Working Groups looking for subject matter experts**
- **Working documents and status for P1735 are maintained at:**
  - **http://www.eda.org/twiki/bin/view.cgi/P1735/WebHome**

Our Contribution

- **Document recommended practices with detailed use cases and necessary pragma changes to enable effective use of IP protection**
- **clarify omissions, make interpretations, and correct errors in P1800 and 1076 by liaison**
- **recommend revisions to the "Protected Envelopes" clause.**
  - **At minimum the changes will consist of inter-operability resolutions**
  - **There is a possibility of more extensive changes to improve readability and precision**
- **define new or revise existing pragma syntax to enable use models as required**
  - **Syntax and necessary semantics go into P1800**
  - **Use model details are a P1735 work product**
- **recommend enhancements to introduce a rights management and licensing framework**

Implications

- P1735 is not re-factoring the LRMs into a common specification
- We will lead on the language independent aspects
- P1800 has to vet and incorporate the inputs
  - Continuing the relationship and process used to address the “initial vector” problem in 1800-2009
  - This discussion should give you a feel for the scope
- The language specific issues are yours
  - This discussion has our requirements
  - We’ll work with you

Outline

- **Interoperability**
- **Rights Management**
- **Licensing**
- **Visibility**
- **Flow Issues**

Basic Interoperability

- **The specified IEEE encryption isn't interoperable for minor reasons**
- **P1735 has a set of recommendations to resolve ambiguities and errors that affect IP exchange between vendor tools**
- **Recent changes to export control regulations enable us to revisit the required algorithms list**
- **Working group unanimous approval of version 1, which is roughly equivalent to a draft standard**

Version 1 Recommendation

- **Digital envelope use model with required algorithm support**
- **Pragma versioning to manage conformance and backward compatibility**
- **Syntax errata for 1800-2009 and 1076**
- **Clarification of default behavior for tools that produce derivative outputs like synthesis**

Rights Management

- **The primary objective of rights management is IP author control over tool functionality in the flow**
  - **Example: Distributing protected IP that is freely available for simulation, but needs further rights for synthesis and layout**
- **Licensing is viewed as a subset of rights that are granted to specific users**
  - **Needs to be integrated as part of the overall rights specification**
  - **Current license pragma is insecure and not feature oriented**

P1735 Licensing Model

- External Model (required)
  - Secure RPC or client/server model
  - IP author provides/obtains compliant licensing technology
  - Reference implementation TBD
- Internal Model (optional)
  - Relies on tool vendor licensing technology
- Use cases, license verification, detailed comparision of models in P1735 WG Twiki

IP Visibility

- There are basic semantics at the 30K ft level
  - hide everything
  - with enough visibility for tools to satisfy their purpose
- The underlying VPI information model has a few details
  - a protection flag for objects
  - some semantics for access/navigation
- IP author controls are limited
  - Disjoint protected envelopes
  - Viewport is a markup syntax placeholder in SV for proprietary use
  - portable feature in VHDL

What's Wrong With That?

- **Important tool outputs are not considered**
- **The information model only considers the 1364 subset of SV**
  - **A basic non-trivial effort is needed**
  - **more use cases than VPI access at stake**
- **Portable visibility control is needed**
  - **Use of protected IP has to be debug able**
  - **Configuration, binding SVAs, disjoint protected regions, other flow issues…**

Tool Outputs

- **What should assertions embedded in IP do when they fire?**
  - **Be silent, be cryptic, be transparent, be controllable by the IP author?**
- **Can coverage be gathered and reported within protected IP?**
- **Error and Warning message issues matter**
  - **IP is rotten to the core**
  - **It has to be possible for the IP user to get tool vendor/IP author support while protecting their own proprietary data**

A closer look at the information model and protected HDL

- IM needs to be well formed and there are missing protection semantic rules
  - The protect pragmas can be applied to any lexical subset of an HDL model
  - What semantic rules should govern partially protected constructs?
    - Is a partially protected composite type reasonable?
    - Hiding data members and methods?
    - Hrefs across disjoint protected regions?
- IM protection semantics should serve more than just PLI
  - Should tool outputs and error messages have their defined access in the IM?

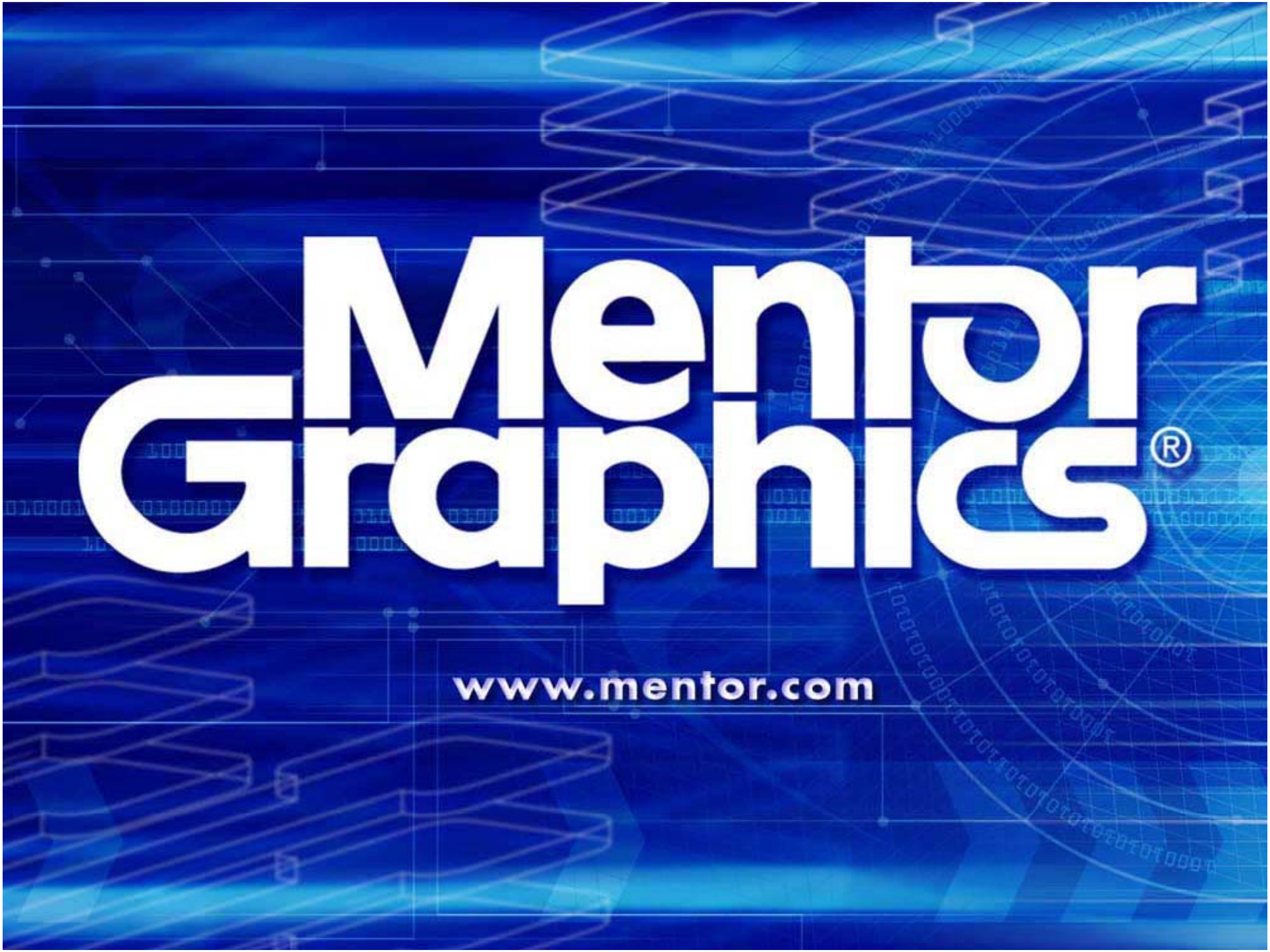
Some Flow Issues Go Beyond 1800

- **Can I bind or annotate anything into protected IP if I am given enough information (default implicit visibility rule) ?**
  - **i.e., should there be default implicit visibility rules**
- **Do SDF files need to be generated in an encrypted form for protected blocks?**
- **Is a tool expected to annotate unprotected SDF to an encrypted region?**
- **What's the access implication of the power supply network of a UPF power region that contains protected IP?**

<u>P1735 needs more collaboration on such issues</u>

Summary

- **We'll have inputs to be incorporated**
- **You should focus on visibility, an improved formal information model, and deal with tool outputs**
- **Please make your next PAR broad enough to include all this**


Mentor Graphics®
www.mentor.com

Basic IP exchange

Tools providing basic IP exchange consistent with this recommendation shall support the following changes to the standards:

1. **In the defined identifiers table associated with the data_method pragma keyword, replace the *Encryption algorithm* portion of the description for the "rsa" encryption algorithm with "RSAES-PKCS1-v1_5, see IETF RFC 3447".**
2. **Replace IEEE Std1800-2009 key_block description with a restatement of key_block content from IEEE Std1076-2008.**
3. **<new> Extend IEEE Std1076-2008 to require key_public_key block be supported to accept public keys in the HDL input to encryption tools.**
4. **Extend IEEE Std1800-2009 to require key_block support in the encryption envelope for specifying additional key blocks.**

Tools which transform data protected by a decryption envelope shall document the protection mechanism used for data derived from the decryption envelope. If the tool claims basic IP exchange conformance for the output, the session key used for the derived data must be identical to that of the decryption envelope from which it is derived. As a further restriction, the set of key blocks that apply to the derived data shall be a subset of those that apply to the data from which it is derived.

A version pragma value of no less than 1 shall be used to mark protected envelopes for encryption and/or decryption under basic IP exchange rules.