Corrections to the Encryption Flow description in IEEE Std 1076-2008

Add “protect key_public_key” directive description.
This directive is required to specify public key of the vendor authorized to receive session key used in data block encryption.

The directive should be used in encryption envelopes only.

Clarify IV handling in CBC mode.
Initialization Vector (IV) is required by symmetric ciphers and should be generated randomly for each session and can be transmitted with the encrypted message without additional protection.

1076-2008 does not specify how to handle IV used for encryption of data block with symmetric ciphers working in CBC mode. Appropriate explanation should be added to the description of “protect data_block” directive, and possibly to the description of supported ciphers.

Method described in 1800-2009 should be copied: “After encryption, IV used in the process should be prepended at the beginning of the encrypted data block right before the encoding of the entire block. In the decryption tool, IV should be removed from the beginning of decoded data block and used for the final decryption.”

Ambiguous Triple DES description

Current standards mentioned above describe two Keying Options that differ in the number of unique keys used in three DES rounds. Updated VHDL standard should clearly indicate that only Keying Option 1 (three unique keys) should be used.

Ambiguous RSA description
Current description of RSA public key cipher is ambiguous. To clarify which padding scheme should be used, updated VHDL standard should mark RSA as described in “RSAES-PKCS1-v1_5, see IETF RFC 3447”.

Missing data block padding description
Symmetric cipher standards and HDL standards do not specify how to pad plaintext message to the nearest multiplicity of the cipher block size. Updated VHDL standard should require PKCS5 padding scheme (add n bytes of value n).