I sent comments to the TC for the public review:


Looking at the message in the email archive results in a lot of garbage, so I will try to insert the corrected message below, if I can work around Jira's formatting idiosyncrasies.

While preparing csd01 for publication, OASIS staff noted several issues which should be addressed.

The line numbers listed below are in the published DOCX or PDF documents:

- [https://docs.oasis-open.org/pkcs11/spec/v3.1/csd01/pkcs11-spec-v3.1-csd01.docx](https://docs.oasis-open.org/pkcs11/spec/v3.1/csd01/pkcs11-spec-v3.1-csd01.docx)
- [https://docs.oasis-open.org/pkcs11/spec/v3.1/csd01/pkcs11-spec-v3.1-csd01.pdf](https://docs.oasis-open.org/pkcs11/spec/v3.1/csd01/pkcs11-spec-v3.1-csd01.pdf)
  
  There are also some references to line numbers in the HTML format, which does not display line numbers unless examined in a text editor:
- [https://docs.oasis-open.org/pkcs11/spec/v3.1/csd01/pkcs11-spec-v3.1-csd01.html](https://docs.oasis-open.org/pkcs11/spec/v3.1/csd01/pkcs11-spec-v3.1-csd01.html)

1) Line 14589 - Appendix B contains a statement which contradicts OASIS policy, by asserting that some files located in github which are not included with the published document are normative:

"The definitions for manifest constants specified in this document can be found in the following normative computer language definition files:


This appendix should be modified in one or both of the following ways:

- instead of referring to github, provide a link to the files referenced in "Additional artifacts" (the Word document already has a bookmark for this purpose)
- refer to the github files as "latest versions published in the PKCS11 TC repository" or something similar.

2) Broken or unusable references.
We corrected many incorrect reference links during publication (if interested, these are listed in the JIRA ticket [https://issues.oasis-open.org/browse/TCADMIN-4164](https://issues.oasis-open.org/browse/TCADMIN-4164)). The TC should correct the following links in future publications.

- [SEED] - line 257 - link only displays some short text in Korean
- The links provided for PKCS # (1, 3, 5, 7, 8, 12) (lines 217 +) are not hyperlinked. The TC should either explain that these are historical links which no longer function, or find correct links. Also, note that for the PKCS RFCs included here, the actual version numbers don't match the listed titles in some cases. If possible, the TC should investigate which accessible sources are currently relevant for the purposes of this specification.

3) Broken link, incorrect reference format:
Section 6.46, line 12522 - The reference hyperlink is broken" (D:\blp\data\http:\www.counterpane.com\twofish-brief.html") and does not match the visible text. Also, this should point to a document listed in the References section.
4) Some occurrences of the "less-than or equal" sign are corrupted and should be replaced. In browsers like Firefox, this shows up as a pound sterling symbol. This is a historical issue, largely due to copying text from older documents created with older versions of Microsoft Word, dating back to at least 2013 in the DOC format. There are a large number of occurrences of this issue, mostly within tables:

NOTE - the line numbers listed in square brackets are the line numbers where the "£" appears in the HTML code:

Table 35 - DOCX/PDF line 6517 - eight occurrences
[- 29483 - 29522 - 29549 - 29582 - 29615 - 29654 - 29681 - 29720]
Table 38 - line 6580 - four occurrences
[- 30101 - 30131 - 30151 - 30181 ]
Table 40 - line 6639 - four occurrences
[30443, 30471, 30499, 30533]
Section 6.1.12 - one occurrence - DOCX line 6662
[30588]
Table 41 line 6678 - six occurrences
[30662, 30713, 30739, 30765, 30816, 30848]
Table 42 - Line 6705 - two occurrences
[30957, 30982]
Table 46 - Line 6812 - four occurrences
[31516- 31549- 31570- 31607]
Table 47 - Line 6841 - four occurrences
[- 31707- 31737- 31757- 31787]
Table 71 - Line 7661 - one occurrence
[- 37162]
Table 72 - Line 7681 - one occurrence
[- 37288]
Table 74 - Line 7701 - one occurrence
[- 37563]
Table 75 - Line 7719 - one occurrence
[- 37703]

Description of issue:

- The symbol used for "less-than or equal" in older (or possibly older British-English) versions of Word is confused with the pound sterling symbol in Word. This shows up in particular when Word saves the document as HTML, where the HTML code is generated as:
  `<span style='font-family:Symbol'>£</span>`
  instead of one of the expected HTML codes for "less-than or equal" such as:
  ```html
  ≤
  ```

Some browsers such as Chrome or Microsoft Edge translate the pound sterling symbol to "less-than or equal", while others display the pound sterling in the mathematical formula. See for example the 2013 document:


And similarly in the current document:

- [https://docs.oasis-open.org/pkcs11/pkcs11-spec/v3.1/csd01/pkcs11-spec-v3.1-csd01.html#_Toc98177224](https://docs.oasis-open.org/pkcs11/pkcs11-spec/v3.1/csd01/pkcs11-spec-v3.1-csd01.html#_Toc98177224)

- If viewed in the Firefox browser, the tables show that the expected "≤" has been replaced by "£".
Solution: While editing the document in Word, replace the old "corrupted" symbols with new symbols, using "Insert Symbol".
(Verify by generating HTML and examining the representation.)

5) somewhat related to the previous issue (4). This only occurs in Table 40, line 6639. The symbols "[" and "]" (floor or "round down") are replaced by "ë" and "ü" in some browsers, including Firefox. Again, these symbols were apparently carried over from older publications, and should be replaced using a current version of Word. I think the easiest way to obtain these characters is using "alt-codes":

- left floor is 8970, and right floor is 8971.
- With "Num Lock" on, hold the Alt key down and use the numeric keypad to enter the digits, then release the Alt key.

6) There are several (apparently 16) places where the two symbols "\leq" are used instead of "\le". The document should use one or the other formats consistently. There are two places (both in Table 189 at line 11104) where "\geq" is used.