SSL Standardization Subcommittee teleconference minutes 05/14/2003

Attendance:

Frank Farber – TMC (DCC Chair)
Jody Fromer - Lubrizol
Doni Grande - Ethyl
Mark Griffin – SwRI (Scribe)
Dave Hood - Chevron Oronite (SSL Chair & editor)
Mike Kahn - Chevron Oronite
Sally Lloyd - Perkin Elmer
Bill Mahoney – RSI/ERC
John Rivenburgh - Perkin Elmer

Convened:

11:00am PDT

Agenda Items:

- Intro
- Review of last meeting Individual Updates
  - Include work done
  - ID issues
  - next steps
- Review attached ETRTM and related SSL documentation for the DCC standard
- Next Steps for SSL SSC

Dave Hood asked for any changes/additions to the agenda, none were given.

Review Meeting Minutes / Action Items:

The meeting minutes (for the SSL-SSC) were reviewed from the 04/02/2003 tele-conference. No changes were made, minutes were approved.

The action items were reviewed. Re: company updates for current status.

Company updates on SSL status:

Chevron Oronite

Dave Hood reported that Chevron Oronite had nothing to add (since last meeting); there has been no change in hardware or software. The development of the

rough draft of the SSL outline for the ETRTM has been completed and sent out to all SSL-SSC members for review / feedback. Dave said that he had received some feedback.

ERC / RSI

Bill Mahoney reported that they (RSI) have made contact with Gordon Farnsworth to initiate discussions concerning the adoption/ inclusion of the ACC COP form and fields into ACC test type data dictionaries.

Bill also reported that beta testing for North American testing labs has been delayed, but expects a mid to late June start up. Bill indicated that the RSI site would be a replication of what is being used on the European side.

Lubrizol

Jody Fromer reported that a site is officially ready for production, that they have completed preliminary testing with SR, and plan to begin testing with PE very soon.

Ethyl

Doni Grande stated that there was nothing new to report. Doni said that they have looked at it and should have no problems doing it (the SSL work).

Infineum

Dave may have had a bad email address for Lika, but has discussed issues raised during this teleconference with her.

Infineum has completed the design of their SSL application and estimate production to be complete sometime in the 3rd quarter of 2003.

TMC

Frank Farber reported that the TMC is going through server upgrades and expects to begin (SSL work) in the late summer (July / August) time frame. The TMC will offer this (SSL) as a replacement for the current transmission method.

Labs (PE & SR)

PE – Sally Lloyd reported that they are doing fine, nothing to add.

SR - Mark Griffin reported that they have tested three secure sites all using HTTP/S and forms based uploads/downloads, two in production and one in preparation for production (user training). All is going well, no problems to report. Mark also

reported that some trading partners have indicated a need to use secure FTP, which could also be achieved using SSL.

Review of Draft:

The drafts were distributed as 2 documents, one refereeing to the other. The first addresses proposed changes to Section 3 of the ETRTM. The second (Appendix I) provides general guidelines for architecture and implementation.

ETRTM: Section 3

Original proposal discussed at teleconference

3.0

All Flat Files shall be transmitted to the receivers via Internet Secure Sockets Layer (SSL) protocol or Internet File Transfer Protocol (FTP). Please note that FTP is not a secure protocol therefore SSL is preferred for proprietary data. Most WEB browser and server products include SSL. Refer to Appendix I for more detail on SSL implementation.

Dave Hood stated that they had removed all of the X.400 references in section 3.0 and removed section 3.1 entirely.

Mark Griffin suggested that since SSL is actual a protocol for the secure layer and not the application layer, that the wording be changed to include the two available application protocols HTTP/S and FTP/S that could be run on top of the security layer.

Mark Griffin also commented that the wording in the sentence that mentions the Web browser could be changed to refer to an "SSL-enabled browser" (to borrow from existing computer terminology).

Frank Farber requested that email (SMTP) could be mentioned (as a non secure method).

New proposal based on teleconference discussion:

3.0

All Flat Files shall be transmitted to the receivers via (a) Internet HTTP/S or FTP/S applications using the Secure Sockets Layer (SSL) protocol, or (b) via standard Internet File Transfer Protocol (FTP) or Simple Mail Transfer Protocol (SMTP). Please note that both FTP and SMTP are not secure protocols therefore SSL usage is preferred for proprietary data. SSL-enabled browser and server products are commonly available. Refer to Appendix I for more detail on SSL implementation guidelines with an example using HTTP/S.

ETRTM: Appendix I

The attached Word document is the original proposal discussed at the teleconference.

ssl_appndx.doc (36 KB)

Dave asked for suggestions to replace the term "sniffed". Frank Farber suggested changing the word to "compromised". All agreed.

Bill Mahoney raised a concern that the wording may be exclusionary for companies that have already established an SSL secure website solution. Bill suggested that the document focus on function instead of form. The group present at the meeting agreed that the wording used should reflect that these are recommended guidelines to be treated as suggestions. This was deemed useful for the first time users.

Frank Farber suggested changing the word "basic" to "recommend" in the file hierarchy sentence. All agreed to this change.

Dave mentioned his concern about the use of specific software vendors in a DCC document. He stated that he would re-word the text used in the Implementation Example to replace references to IIS and SAFileUp with general descriptions of the products.

Dave stated the use of product names such as Verisign and SiteMinder were well known and used throughout commercial websites and did not see those as much of an issue. Again, all agreed to these changes.

The attached Word document is the new proposal with changes discussed at the teleconference.

ssl_appndx1_.doc

Closing remarks:

Dave Hood assigned follow-up work for the suggested editorial corrections to the draft, to be completed by Friday 5/16/2003.

Appendix I Dave Hood

Section 3.0 Mark Griffin

Next Steps:

1) Dave Hood will distribute the new proposed drafts along with the meeting minutes to the SSL-SSC members.

2) A two-week period will be allowed for review and then the draft will be released to the DCC chairman if there are no issues raised. The document will be proposed as text to be included in the ASTM DCC 2 weeks from today's release date of these proposed changes is: 5/29/03.

3) Dave Hood will call another SSL-SSC teleconference to resolve any issues with the proposals. If there are none we will proceed to Step 4 of "Next Steps". Otherwise we will continue to recycle "Next Steps" 1 thru 3 until all issues are resolved at which point Dave will notify Frank to initiate Step 4.

4) Frank Farber will conduct a DCC tele-conference call to call for a vote on approval for the ETRTM changes and the addition of Appendix I.

Adjourned:

12:05pm PDT