

May 4, 2007

## Report of the **DSEC Telecon 10** held on **2 May 2007**

In attendance were:

Doug Murri, Southwest	Paul Storck, ARINC
Greg Danforth, USAF	Dave Coombs, Carillon
Frank King, USAF	Mike Olive, Honeywell
Cindy Freud, USAF	Lou Toth, Honeywell
Hugh Mote, Airbus	Alain Bothorel, Rockwell Collins
Mathias Julien, Airbus	Eric Mehn, SITA
Derek Schatz, Boeing	Mike Russo, IA Staff

Mike Russo opened a one-hour forty minute teleconference. The primary topics were the status of the re-organized Part 1 to Project Paper 823. The telecon also discussed of intellectual property rights issues (with regard to the acceptability of PP823 for adoption) and the status of action items to progress the drafting of new sections of PP823. This teleconference was held from 1500 - 1640 UTC.

Secretary Mike Russo introduced the proposed agenda.

<b>Telecon 10 Agenda</b>		<b>2 May 2007</b>
	<b>Description</b>	<b>Documents</b>
1	Admin: Report of Telecon 9 / Action Item Status	Report of Telecon 9
2	An Overview of the Restructured Part 1 of PP823	Table of Contents - HI
3	Test Vectors (Part 1 Appendix): location of vectors; scripting	
4	Content or bullets for Action Item deliverables	
5	Status of PP823 Part 2 Development	
6	Placeholder for discussion of non-patented approach	AEEC Position Paper
6	Close	

### **Introduction**

Doug Murri chaired the meeting but had to leave early for another commitment. Mike Russo opened the teleconference with introductions. He quickly summarized the previous telecon, noting that not been well attended due to an error in the e-mail distribution to the DSEC mail list. On request he reopened the AEEC Position Paper developed at the AEEC Mid-Term meeting. He noted that the AEEC had established directives for the DSEC SC that it should:

1. Evaluate non-patented alternatives for PP823
2. If the patented techniques were best, then explain the advantages to AEEC
3. provide assurances that if ARINC 823 were to contain patented functionality that it would be implemented.

Mike went on to poll members on the status of outstanding action items.

A.I. -2-07\_20: Alain Bothorel asked that DSPs provide additional PICs to support internetworking. Eric Mehn reported that correspondence between SITA and ARINC has begun, but no progress has been made yet. SITA management views the reciprocity feature in the pro forma license as a potential barrier to adoption of PP823 and therefore it has become difficult to obtain the resources necessary to complete the work on this task.

A.I. -2-07\_22: Mathias Julien reported that arrangements have been made for him to coordinate the diagram and the text by 16 May. He predicted that his action item could be closed at the next meeting.

A.I. -2-07\_23: Dave Coombs reported that he had completed his action. Mathias is working on the text for Section 4.0 of Part 2 that was assigned to Stephane Tamalet.

A.I. -2-07\_24: Mathias reported that progress is being made toward completion of this task and that an input should be available for review at the next DSEC SC meeting.

### **An Overview of the Restructured Part 1 of PP823**

At the previous meeting, the DSEC Subcommittee directed its industry editor to merge Parts 1 and 3 of PP823. Mike Olive presented a copy of the table of contents for the re-structured Part 1 of PP823. Mike's table of contents had been highlighted to distinguish among:

- 1) text derived from the old Part 1 – primarily Appendix B of the new Part 1
- 2) text that had resulted from a merger of definitions from Part 1 and Part 3
- 3) new text that was recommended by the previous meeting and associated action items.

One of the new aspects introduced at the previous meeting was to add PICs. The list of PICs provided by Rockwell Collins France and SITA will be included in Appendix G. The PICs apply to 4 configurations:

1. Public/Private key processed by DSP
2. Public/Private key processed by end user
3. Shared Secret key processed by DSP
4. Shared Secret key processed by end user

Appendix H will contain test vectors. A complete copy of the revised PP823 Part 1 will be circulated to the DSEC e-mail list in about one week.

### **Status of PP823 Part 2**

Mike Olive reported that all of his efforts had been directed to the reorganization of Part 1 and that no significant progress had been made toward completion of Part 2. New text addressing the shared secret key will be included as the material becomes available. There was no discussion.

### **Status of Licenses for Honeywell Patent**

Although the status of the Honeywell patent was discussed at the previous telecon, many of the participants had not been in attendance. Mike Russo reported that, at their Mid-Term meeting in April, AEEC discussed the conditions of the Honeywell Commitment to License at length. The result was an AEEC Position Paper with guidance to the DSEC Subcommittee. In summary, AEEC is not favorably disposed toward adopting standards that contain provisions that are subject to any patent. They asked that the DSEC SC revisit their decision to include such provisions and if the patented technology is re-selected, a rationale for the decision should be provided to AEEC. And, AEEC asked for feedback from potential licensees that they would be willing to implement the

security functions as defined in PP823. Mike Russo noted that Don Shell, Honeywell, had announced that Honeywell also has an application for a second patent that, if granted, would apply to PP823 in its current form. Such disclosure is the first point of the AEEC patent policy. DSEC members on the telecon were curious to know the scope of coverage of the second patent. Lou Toth promised to ensure that a patent status overview was provided to the members at the next DSEC meeting.

Mathias Julien offered to provide his analysis, from an Airbus point of view, of the technical applicability of the Honeywell patent. While not a legal expert, he has developed some questions regarding the conditions of license. Mathias asked that others with questions submit them to form a consolidated list. These observations/questions will be circulated to the DSEC mail list and discussed at the next DSEC meeting.

### **Circulation of PP823 Part 1**

Mike Olive reported that he will submit the strawman of Part 1 of PP823 (restructure) within a week. Telecon participants asked that the file be sent to the DSEC list in addition to posting on the DSEC web page.

### **Next Meeting**

The next meeting (DSEC7) is scheduled to be held on 5-7 June in Annapolis, Maryland.

This report was prepared by Mike Russo, IA Staff.

**ATTACHMENT 1  
LIST OF ACTION ITEMS**

<b>Table 1: Action Items – Meeting 1, January 2006 Meeting</b>		
<b>#</b>	<b>DESCRIPTION</b>	<b>STATUS</b>
01-06_01 – 04		Closed 3/21/06

<b>Table 2: Action Items – Telecon 1, 15 February 2006</b>		
<b>#</b>	<b>DESCRIPTION</b>	<b>STATUS</b>
02-06_05-06		Closed 3/21/06

<b>Table 3: Action Items – Meeting 2, 21-23 March 2006</b>		
<b>#</b>	<b>DESCRIPTION</b>	<b>STATUS</b>
03-06_07 03-06_09		Closed 11/29/06
03-06_08	Mike Russo will explore the viability of tagging requirements in ARINC Standards with AEEC members. Julien Touzeau will provide an example for sharing with members. <b>Mike Russo will present this to AEEC at its <del>on</del> via e-mail.</b>	Open

<b>Table 4: Action Items – Meeting 3, 23-24 May 2006</b>		
<b>#</b>	<b>DESCRIPTION</b>	<b>STATUS</b>
05-06_10-12		Closed 2/27/07

<b>Table 5: Action Items – Telecon 4, 12 July 2006</b>		
<b>#</b>	<b>DESCRIPTION</b>	<b>STATUS</b>
07-06_13-14		Closed

<b>Table 6: Action Items – Telecon 5, 4 October 2006</b>		
<b>#</b>	<b>DESCRIPTION</b>	<b>STATUS</b>
10-06_15		Closed 12/18/06

**ATTACHMENT 1  
LIST OF ACTION ITEMS**

<b>Table 7: Action Items – Meeting 5, 29 November 2006</b>		
#	DESCRIPTION	STATUS
11-06_16		Closed 02/28/07

<b>Table 8: Action Items – Telecon 7, 17 January 2007</b>		
#	DESCRIPTION	STATUS
01-07_18-19		Closed 02/27/07

<b>Table 9: Action Items – Meeting, 27 February – 1 March 2007</b>		
#	DESCRIPTION	STATUS
02-07_20	<b>Eric Mehn and Debbie Jacobs</b> will assess the potential need for additional mechanisms to support internetworked air-ground encrypted messages, i.e., where there is a handoff from the initiating DSP to another DSP (where the DSP that is connected to the user does not support security for that user) for message delivery. See Honeywell Comment Disposition C-1 p150 Note 5. <b>Alain Bothorel</b> will define PICs to support the internetworking functionality and any new provisions required by the avionics.	Open
02-07_21		<b>Closed 02/28/07</b>
02-07_22	<b>Mathias Julien</b> will revise text of Section 3.4.6 and Figure 3.5-1 of PP823 Part 1 to clarify the ability of a user to turn off any security provisions. This feature is needed in certain localities where the government restricts the use of security.	Open
02-07_23	<b>Michael Leonard</b> and <b>Dave Coombs</b> offered to assist Mike Olive in expanding the content of Section 3.1, Asymmetric key Management, and Section 3.2, Key Management Life Cycle of Part 2. Stephane Tamalet offered to provide an equivalent input for Section 4.0, Symmetric Key Management.	Open
02-07_24	<b>Cecile Morlec</b> will provide a report of the on the SAFEE compression experiment.	Open

**ATTACHMENT 1  
LIST OF ACTION ITEMS**

<b>Table 10: Action Items – Telecon 10, 2 May 2007</b>		
<b>#</b>	<b>DESCRIPTION</b>	<b>STATUS</b>
<b>05-07_25</b>	<b>Lou Toth promised to ensure that a patent status overview was provided to the members at the next DSEC meeting.</b>	<b>Open</b>
<b>05-07_26</b>	<b>Mathias Julien will share the Airbus view of the technology covered by the Honeywell patent and consolidate his questions with those of other potential licensees. Questions should be submitted to Mathias by 17 May to prepare for the next DSEC SC meeting.</b>	<b>Open</b>