FUJ00078984

PDA QUALITY REVIEW COMMENT SHEET

Section A (To be completed by Author of document)

Document Name	POCL Infrastructure Acceptance Specification
Version Number	1.0
Document Date	23/05/97
Document Author	Dave Cooke
Deadline For Comment	
Comment To Go To	Mary Reade

Section B (To be completed by Reviewer of document)

Reviewer Name	Jeremy Folkes, PDA
Date of Review	03/06/97

Section C (To be completed by Reviewer of document)

No.	Para No. or Ref	Error, Comment, Typo or Omission (Prefix E,C,T,O)	Impact H/M/L/N (High, Medium, Low, Negligible)
1.	General	There seems to be a general reliance on "the Pathway Technical Architecture". Acceptance has to be on something more concrete - either a specific document needs to be created to define this architecture at the right level (not the TED), and/or Pathway need to demonstrate the characteristics. (See the wording in the Introduction of the TED to put this into context).	M
2.	5.2 R472.2	I would expect this to be covered by review as well as trial - Pathway need to demonstrate how compromise is avoided.	M
3.	5.2 R478.14	I would expect this to be covered by review as well as trial - Pathway need to demonstrate the security/completeness/accuracy and robustness of the data transfer. Tests cannot prove these characteristics.	M
4.	5.2 R541.1	The scalability needs to be demonstrated - I know of no existing document which does this.	M
5.	5.2 R558.2	I would expect this to be demonstrated through modelling.	M
6.	5.3 R466.2	*Provision of estimates* does not meet the need for *detailed specifications of all the consumables*	M
7.	5.3 R467.1	The description in the TED is not sufficient to demonstrate this capability.	M
8.	5.3 R467.2	The SFS specifies a number of technical controls, it does not guarantee that the transfer of data is secure, complete, accurate and robust. Reference to these the SFS and Pathway Tech Arch will not be sufficient for acceptance.	M
9.	5.3 R567.3	Don't see how the Riposte 32 API calls will tell us this - the requirement is for the authorities to identify whether or not data has been received; we are unlikely to do this by direct reference to the Rip32 API!	M
10.	5.3 R469.1	I would suggest that this documentation set is not complete as a means to enable procurement of other applications - these would not give sufficient information on how to develop an application for OPS.	M

FUJ00078984

11.	5.3 R469.2	CHDS does not define OPS - the CHDS is therefore insufficient on its own. There is more to OPS than the Counter Hardware.	M
12.	**5.3 R470.1/2**	**The TED is not sufficient as a description of TMS, and even with the SADD it would not be sufficient as a basis for the procurement of applications.**	**M**
13.	5.3 R472.2	Acceptance of the SFS is not sufficient; the SFS only describes particular technical controls on certain aspects of the system. A wider set of documents (including ACP, Security Standards etc), plus documentation on the application and middleware, would be necessary.	M
14.	5.3 R472.3	The TED is not sufficient as a description - this describes aspects of the OPS/TMS message store and archive mechanisms but gives no details on what events are recorded, ie what is audited.	M
15.	5.3 R474 et seq	Depends on the scope of the Declaration of Technical Conformity. To minimise our risk we may require to see proof of conformity for individual aspects, especially regarding H&S.	M
16.	5.3 R476.2	Proof of sufficient and satisfactory testing will need more than acceptance of the Strategy - we will need evidence that it is being followed, that testing does meet these criteria.	M
17.	5.3 R478.8	Is this requirement actually met? I doubt that the TED is sufficient to accept.	M
18.	5.3 R478.9	Is the switching capability actually described in a Riposte document? Surely a central agent would be required to perform this switching, for communication outwith a single group?	M
19.	5.3 R478.9/10/11	Acceptability of this document yet to be assessed - presumably it's not one which was used during the Demo, if so that is unlikely to be of sufficient detail for acceptance, nor current.	M
20.	5.3 R478.12	Referenced documents seem very technical - how will the business functions - financial summaries, reconciliation, etc be accepted through these?	M
21.	5.3 R478.13	As with OPS, acceptance of the underlying mechanisms is insufficient to accept that a "full audit trail" is being logged - we need visibility of what events are being recorded?	M
22.	5.3 R479.2	(This was also covered in the Services spec, but with ref to the ACP!) The SFS does not approve which systems can and can't be connected - for this I would expect the register, as defined in the requirement, to be presented for approval. The SFS would be one means by which we would inform out approval decision. The register, and its associated processes, need to be provided.	M
23.	5.3 R479.5	(Have yet to see evidence of these documents)	L
24.	5.3 R480.1	I would expect to see a description of the logical separability - the references themselves are unlikely to be sufficient. What is the "Service Architecture" - is this the SADD?	M
25.	5.3 R536.2	I would expect this to be demonstrated at the peripheral level - to show that removal and swapping, for instance, could be detected. The Riposte Peripheral Broker is probably at too high a level for this.	M
26.	5.3 R541.1	I would expect evidence and output from modelling, plus paper demonstration of the scalability. Insufficient to rely on "inherent", we need to be shown it!	M
27.	5.3 R555	The CHDS really just confirms the requirements here - we would want some evidence that indeed it does meet the requirements. Although there is no processing of AP Smart txns in Release 1, I would still expect the capability to access the required devices to be demonstrated - to avoid downstream risk.	M
28.	5.3 R922.1	Presumably this would be covered by Pathway's Technical Conformity Statement (and backed up by testing, not just mfgrs spec sheets)	M
29.	5.3 R952.1/2	Much of the key management functionality is not supplied until Release 2 - so acceptance of these may need to be deferred until then. Suggest you may need to include the Crypto Design Spec here, the SFS is unlikely to provide the detail needed.	M

FUJ00078984

30.	5.3 R953.2	Does the Reports and Receipts document cover “integrity”?	M