FUJ00103477

PinICL Export PC0005088

Ref	Summary	Opened	Last update	Customer	Product Group
Logged By		**Closed**	**Status**		**Product At Fault**
PC0005088	CAPS Link Crypto Key Mgmt:	15/07/1997 11:50:02	24/09/1997 15:59:41		Infrastructure
Fallon	restrict role to consol	24/09/1997 15:59:40	C		CAPS Link Crypto

References

Products

Product Group	Product Name	Product Version
Infrastructure	CAPS Link Crypto	

Activities

Date	User	Comment
15/07/1997 10:50:02	[Frank Fallon jun02]	CALL PC0005088 opened
15/07/1997 10:50:02	[Frank Fallon jun02]	Product Security CAPS Link Crypto added
15/07/1997 10:50:02	[Frank Fallon jun02]	Target Release entered: Release 1c
15/07/1997 10:50:02	[Frank Fallon jun02]	CAPS Link Crypto Key Management
15/07/1997 10:50:02	[Frank Fallon jun02]	The Security Functional Specification (Section 8.1.3) states that 'Key
15/07/1997 10:50:02	[Frank Fallon jun02]	material will be loaded locally ... at each end of the CAPS link'.
15/07/1997 10:50:02	[Frank Fallon jun02]	
15/07/1997 10:50:02	[Frank Fallon jun02]	For the Release 1c tests, remote logon was used (as recommended in the
15/07/1997 10:50:02	[Frank Fallon jun02]	Pathway document "Key Management for CAPS Link Crypto Services",
15/07/1997 10:50:02	[Frank Fallon jun02]	PWY/SEC/D/30).
15/07/1997 10:50:02	[Frank Fallon jun02]	Is this method acceptable? At present, there are no remote logon restrictions
15/07/1997 10:50:02	[Frank Fallon jun02]	placed on the CAPS Link "Key Custodian" User Ids.
15/07/1997 10:50:02	[Frank Fallon jun02]	CALL PC0005088:Priority C:CallType T - Target 29/07/97 11:50:02
15/07/1997 10:50:03	[Frank Fallon jun02]	Call transferred to team: TSC-Secure-Dev (Routed via supplied Product name)
15/07/1997 16:33:54	[Roy Birkinshaw oct00]	The agreed method for loading keys is that they should be loaded manually at
15/07/1997 16:33:54	[Roy Birkinshaw oct00]	the console by a trusted person. The document Frank quotes needs to be
15/07/1997 16:33:54	[Roy Birkinshaw oct00]	updated to reflect this. We will do this. It would seem sensible for there to
15/07/1997 16:33:54	[Roy Birkinshaw oct00]	be remote logon restrictions on the CAPS Key Custodian. Is this a

FUJ00103477

Ref	Summary	Opened	Last update	Customer	Product Group
Logged By		Closed	Status		Product At Fault
PC0005088	CAPS Link Crypto Key Mgmt:	15/07/1997 11:50:02	24/09/1997 15:59:41		Infrastructure
Fallon	restrict role to consol	24/09/1997 15:59:40	C		CAPS Link Crypto

15/07/1997 16:33:54	[Roy Birkinshaw oct00]	scripting/roles issue Alan? Regards Roy B
17/07/1997 12:16:30	Alan D'Alvarez	This should be incleuded in Farouk's revision of the Dynix access control
17/07/1997 12:16:30	Alan D'Alvarez	scripts. Can you ask John Lyon to progress this.
17/07/1997 12:16:31	Alan D'Alvarez	The Call record has been transferred to the Team: TSC SecureTest
25/07/1997 10:12:20	[Rob Dick]	Implementation details of the cryptographic design you would like implemented
25/07/1997 10:12:20	[Rob Dick]	on the Sequent platforms at 1c needed within the next two days to meet
25/07/1997 10:12:20	[Rob Dick]	security test deadlines.
25/07/1997 10:12:20	[Rob Dick]	CALL PC0005088:Priority B:CallType T - Target 18/07/97 11:50:02
25/07/1997 10:12:21	[Rob Dick]	The Call record has been transferred to the Team: TSC-Secure-Dev
25/07/1997 12:29:08	[Charles Lambert]	The keychange application on Sequent must be executable only by root. We have
25/07/1997 12:29:08	[Charles Lambert]	been advised by Faruq that the root user can be restricted to only logging in
25/07/1997 12:29:08	[Charles Lambert]	at the console, and we require this. We wish to communicate this
25/07/1997 12:29:08	[Charles Lambert]	"installation" constraint to the relevant parties but do not know who they
25/07/1997 12:29:08	[Charles Lambert]	are.
25/07/1997 12:29:08	[Charles Lambert]	The Call record has been assigned to the Team Member: Charles Lambert
28/07/1997 10:37:55	[Charles Lambert]	F} Response :
28/07/1997 10:37:55	[Charles Lambert]	In conjunction with PC0005021, we will revise the Operating Instructions
28/07/1997 10:37:55	[Charles Lambert]	(initialisation section) for CAPS Sequent Key Management to specify that the
28/07/1997 10:37:55	[Charles Lambert]	key file will be writable only by root, and recommend that the root user be
28/07/1997 10:37:55	[Charles Lambert]	restricted to console acces only. This will effectively introduce a "two-man
28/07/1997 10:37:55	[Charles Lambert]	rule" for key changes: both the root user and the Key Custodian will need to
28/07/1997 10:37:55	[Charles Lambert]	participate. Note that this does not affect routine restarts of the system,
28/07/1997 10:37:55	[Charles Lambert]	when the persistent key store will enable the cryptographic code to start
28/07/1997 10:37:55	[Charles Lambert]	without the presence of either the key custodian or the root user.
28/07/1997 10:37:55	[Charles Lambert]	[END OF REFERENCE 1585384]
28/07/1997 10:37:55	[Charles Lambert]	New target date set 28/07/97 18:00:00

FUJ00103477

Ref	Summary	Opened	Last update	Customer	Product Group
Logged By		Closed	Status		Product At Fault
PC0005088	CAPS Link Crypto Key Mgmt:	15/07/1997 11:50:02	24/09/1997 15:59:41		Infrastructure
Fallon	restrict role to consol	24/09/1997 15:59:40	C		CAPS Link Crypto

28/07/1997 10:37:55	[Charles Lambert]	Responded to call type T as Category 2 -Progress update
28/07/1997 10:37:55	[Charles Lambert]	The response was delivered on the system
28/07/1997 15:03:39	[Charles Lambert]	Our proposed solution requires buy-in from other teams, but it's difficult to
28/07/1997 15:03:39	[Charles Lambert]	discover which ones. I have sent the proposal by email to Rob Dick, John
28/07/1997 15:03:39	[Charles Lambert]	Lyon, Richard Long, Barry Procter and others, and I am awaiting guidance.
28/07/1997 15:04:10	[Charles Lambert]	F} Response :
28/07/1997 15:04:10	[Charles Lambert]	-
28/07/1997 15:04:10	[Charles Lambert]	[END OF REFERENCE 1587030]
28/07/1997 15:04:10	[Charles Lambert]	New target date set 30/07/97 18:00:00
28/07/1997 15:04:10	[Charles Lambert]	Responded to call type T as Category 2 -Progress update
28/07/1997 15:04:10	[Charles Lambert]	The response was delivered on the system
30/07/1997 17:48:54	Martin Bailey	Down graded from B+ to B with agreement of Frank Fallon and Rob Dick
01/08/1997 09:39:22	[Charles Lambert]	Following discussion with Barry Procter (SecurityPolicy team), it seems that
01/08/1997 09:39:22	[Charles Lambert]	the solution proposed in response ref 1585384 (above, dated 28/7) is not
01/08/1997 09:39:22	[Charles Lambert]	practicable.
01/08/1997 09:39:22	[Charles Lambert]	
01/08/1997 09:39:22	[Charles Lambert]	To re-focus efforts on this PinICL, I will paraphrase the original query:
01/08/1997 09:39:22	[Charles Lambert]	"The SFS says that key material will be loaded locally. The Key Management
01/08/1997 09:39:22	[Charles Lambert]	document for CAPS recommends loading it remotely and we were able to do this.
01/08/1997 09:39:22	[Charles Lambert]	Ther reason we were able to do this is that there are no measures to
01/08/1997 09:39:22	[Charles Lambert]	constrain this operation to a local point of access. Is this situation
01/08/1997 09:39:22	[Charles Lambert]	acceptable?"
01/08/1997 09:39:22	[Charles Lambert]	
01/08/1997 09:39:22	[Charles Lambert]	Observations:
01/08/1997 09:39:22	[Charles Lambert]	1) The version of the SFS referred to (v2.0) ism out of date.
01/08/1997 09:39:22	[Charles Lambert]	2) We acknowledge that the version of the "Key Management for CAPS Link

FUJ00103477

Ref	Summary	Opened	Last update	Customer	Product Group
Logged By		Closed	Status		Product At Fault
PC0005088	CAPS Link Crypto Key Mgmt:	15/07/1997 11:50:02	24/09/1997 15:59:41		Infrastructure
Fallon	restrict role to consol	24/09/1997 15:59:40	C		CAPS Link Crypto

01/08/1997 09:39:22	[Charles Lambert]	Crypto Services" needs revision.
01/08/1997 09:39:22	[Charles Lambert]	3) Console services and root access for the Wigan and Bootle sites are
01/08/1997 09:39:22	[Charles Lambert]	expected to be remote in any case, for Technical support.
01/08/1997 09:39:22	[Charles Lambert]	4) Preferred policy is not to allow root access locally at the Wigan and
01/08/1997 09:39:22	[Charles Lambert]	Bootle sites.
01/08/1997 09:39:22	[Charles Lambert]	
01/08/1997 09:39:22	[Charles Lambert]	Barry Procter has agreed to survey current policy about restrictions on local
01/08/1997 09:39:22	[Charles Lambert]	and remote access, and to review this PinICL accordingly.
01/08/1997 09:39:24	[Charles Lambert]	The Call record has been transferred to the Team: SecurityPolicy
19/08/1997 16:44:28	[Barry Procter]	Roy, the meeting with Oracle scheduled today (19/08) was designed to address
19/08/1997 16:44:28	[Barry Procter]	the issues surrounding access to the key file. Are you now in a position to
19/08/1997 16:44:28	[Barry Procter]	resolve this PinICL?
19/08/1997 16:44:29	[Barry Procter]	The Call record has been transferred to the Team: TSC-Crypto-Dev
20/08/1997 09:31:39	[Roy Birkinshaw oct00]	F} Response :
20/08/1997 09:31:39	[Roy Birkinshaw oct00]	Nice try Barry, but yesterday's meeting was about PinICL 5021 and the fact
20/08/1997 09:31:39	[Roy Birkinshaw oct00]	that the CAPSkey files had the wrong file protection mechanisms on it. This
20/08/1997 09:31:39	[Roy Birkinshaw oct00]	PinICL is primarily about whether you can remotely get in as root or whether
20/08/1997 09:31:39	[Roy Birkinshaw oct00]	you have to be local so to do. This requires some work on root's access
20/08/1997 09:31:39	[Roy Birkinshaw oct00]	abilities.
20/08/1997 09:31:39	[Roy Birkinshaw oct00]	We believed that for our key installation and change (when the person so
20/08/1997 09:31:39	[Roy Birkinshaw oct00]	doing would need to collaborate with a root user) that this would HAVE to be
20/08/1997 09:31:39	[Roy Birkinshaw oct00]	done locally. This pinICL was raised to state there was no such local
20/08/1997 09:31:39	[Roy Birkinshaw oct00]	restriction in place. Now it transpires that support (including root access)
20/08/1997 09:31:39	[Roy Birkinshaw oct00]	is required remotely. So two issues: 1/ How do we police that any key change
20/08/1997 09:31:39	[Roy Birkinshaw oct00]	is done locally (Perhaps we just say procedurally it has to be so)
20/08/1997 09:31:39	[Roy Birkinshaw oct00]	2/ What is the policy regards root access? (Note crypto team are not involved

FUJ00103477

Ref	Summary	Opened	Last update	Customer	Product Group
Logged By		Closed	Status		Product At Fault
PC0005088	CAPS Link Crypto Key Mgmt:	15/07/1997 11:50:02	24/09/1997 15:59:41		Infrastructure
Fallon	restrict role to consol	24/09/1997 15:59:40	C		CAPS Link Crypto

20/08/1997 09:31:39	[Roy Birkinshaw oct00]	in 2, except for its impact on 1. Regards Roy
20/08/1997 09:31:39	[Roy Birkinshaw oct00]	[END OF REFERENCE 1719041]
20/08/1997 09:31:40	[Roy Birkinshaw oct00]	Responded to call type T as Category 2 -Progress update
20/08/1997 09:31:40	[Roy Birkinshaw oct00]	The response was delivered on the system
20/08/1997 09:31:40	[Roy Birkinshaw oct00]	The Call record has been transferred to the Team: SecurityPolicy
26/08/1997 09:44:21	[Barry Procter]	F} Response :
26/08/1997 09:44:21	[Barry Procter]	Having discussed this with Alan D'Alvarez, he stated that Secure test are
26/08/1997 09:44:21	[Barry Procter]	creatively interpreting the SFS. Version 2 of the SFS, para 8.1.3.1,
26/08/1997 09:44:21	[Barry Procter]	actually states 'Key Material supplied from the Key management System (KMS)
26/08/1997 09:44:21	[Barry Procter]	will be loaded MANUALLY into the Series 39 (VME)and Sequent platforms at each
26/08/1997 09:44:21	[Barry Procter]	end of the CAPS links,'
26/08/1997 09:44:21	[Barry Procter]	
26/08/1997 09:44:21	[Barry Procter]	This is the case. Please close.
26/08/1997 09:44:21	[Barry Procter]	[END OF REFERENCE 1746118]
26/08/1997 09:44:21	[Barry Procter]	Responded to call type T as Category 12 -Answered
26/08/1997 09:44:22	[Barry Procter]	The response was delivered on the system
08/09/1997 09:45:14	[Frank Fallon jun02]	Apologies for creatively interpreting the SFS, but in response to the earlier
08/09/1997 09:45:14	[Frank Fallon jun02]	PinICL 5048 you stated:
08/09/1997 09:45:14	[Frank Fallon jun02]	
08/09/1997 09:45:14	[Frank Fallon jun02]	"CFM will have no requirement for (inter)active operational access to the
08/09/1997 09:45:14	[Frank Fallon jun02]	VME machine. The only access required will be for the CFM
08/09/1997 09:45:14	[Frank Fallon jun02]	Encryption Key Custodian to load keys periodically at the
08/09/1997 09:45:14	[Frank Fallon jun02]	command line. This requires a visit to the DSS ACC as at present".
08/09/1997 09:45:14	[Frank Fallon jun02]	
08/09/1997 09:45:14	[Frank Fallon jun02]	I took this to mean that keys would be entered locally (and manually).
08/09/1997 09:45:14	[Frank Fallon jun02]	Is the procedure different at the two ends of the CAPS link?

FUJ00103477

Ref	Summary	Opened	Last update	Customer	Product Group
Logged By		Closed	Status		Product At Fault
PC0005088	CAPS Link Crypto Key Mgmt:	15/07/1997 11:50:02	24/09/1997 15:59:41		Infrastructure
Fallon	restrict role to consol	24/09/1997 15:59:40	C		CAPS Link Crypto

08/09/1997 09:45:15	[Frank Fallon jun02]	The Call record has been transferred to the Team: SecurityPolicy
12/09/1997 15:35:20	[Barry Procter]	F} Response :
12/09/1997 15:35:20	[Barry Procter]	Alan D'Alvarez has reported that at a meeting held 11 Sept. with Rob Dick and
12/09/1997 15:35:20	[Barry Procter]	Pete Dreweatt, it was agreed that the Key processes document and the
12/09/1997 15:35:20	[Barry Procter]	associated OPINS would be the vehicle to drive the processes for secure
12/09/1997 15:35:20	[Barry Procter]	installation of Keys. These are currently being agreed with the PDA.
12/09/1997 15:35:20	[Barry Procter]	
12/09/1997 15:35:20	[Barry Procter]	This PinICL can be closed as the test has fulfilled it's role of highlighting
12/09/1997 15:35:20	[Barry Procter]	areas that need to be covered.
12/09/1997 15:35:20	[Barry Procter]	[END OF REFERENCE 1879162]
12/09/1997 15:35:20	[Barry Procter]	Responded to call type T as Category 12 -Answered
12/09/1997 15:35:20	[Barry Procter]	The response was delivered on the system
16/09/1997 09:13:52	[Frank Fallon jun02]	The 'associated OPINS' document states that, for the CAPS link:
16/09/1997 09:13:52	[Frank Fallon jun02]	"Two trusted individuals are required to be present at each end of the link.
16/09/1997 09:13:52	[Frank Fallon jun02]	An administrator..... and a key custodian..(to perform)..the key change".
16/09/1997 09:13:52	[Frank Fallon jun02]	
16/09/1997 09:13:52	[Frank Fallon jun02]	This means that (for cryptographic key management) there is no requirement
16/09/1997 09:13:52	[Frank Fallon jun02]	for remote logon to VME. Correct?
16/09/1997 09:13:54	[Frank Fallon jun02]	The Call record has been transferred to the Team: SecurityPolicy
16/09/1997 13:54:19	[Barry Procter]	Al, (correct me if I'm wrong, and I don't want to pre-empt the key management
16/09/1997 13:54:19	[Barry Procter]	opins) my understanding is still that the CFM encryption key custodian will
16/09/1997 13:54:19	[Barry Procter]	load the VME-end of the key locally.
16/09/1997 13:54:20	[Barry Procter]	The Call record has been transferred to the Team: TSC-Crypto-Dev
16/09/1997 14:04:22	Lionel Higman	The Call record has been assigned to the Team Member: Roy Birkinshaw
16/09/1997 14:33:25	[Roy Birkinshaw oct00]	Alan: Lionel did not even read Barry's question before routing it to me so
16/09/1997 14:33:25	[Roy Birkinshaw oct00]	here it is back.

FUJ00103477

Ref	Summary	Opened	Last update	Customer	Product Group
Logged By		Closed	Status		Product At Fault
PC0005088	CAPS Link Crypto Key Mgmt:	15/07/1997 11:50:02	24/09/1997 15:59:41		Infrastructure
Fallon	restrict role to consol	24/09/1997 15:59:40	C		CAPS Link Crypto

16/09/1997 14:33:26	[Roy Birkinshaw oct00]	The Call record has been assigned to the Team Member: Alan D'Alvarez
16/09/1997 18:06:47	Alan D'Alvarez	Barry, this is correct for the VME end of the link. The issue surrounding
16/09/1997 18:06:47	Alan D'Alvarez	how the corresponding Key is loaded onto the Sequent seems to be the debate.
16/09/1997 18:06:47	Alan D'Alvarez	We need to urgently agree the solution with the PDA (Jeremy Foulkes)and I
16/09/1997 18:06:47	Alan D'Alvarez	have mailed him for his comments. Please retain on your stack until I have
16/09/1997 18:06:47	Alan D'Alvarez	an answer.
16/09/1997 18:06:48	Alan D'Alvarez	The Call record has been transferred to the Team: SecurityPolicy
17/09/1997 14:15:10	[Barry Procter]	F} Response :
17/09/1997 14:15:10	[Barry Procter]	Frank, Please disregard Alan's previous note. The subject of Key
17/09/1997 14:15:10	[Barry Procter]	installation is one that will be agreed with the PDA when reviewing the Key
17/09/1997 14:15:10	[Barry Procter]	processes document and associated operating instructions. With regard to
17/09/1997 14:15:10	[Barry Procter]	your query, I can confirm that the Key will be installed locally at the VME
17/09/1997 14:15:10	[Barry Procter]	end of the link. I hope this is sufficient to clear this PinICL and progress
17/09/1997 14:15:10	[Barry Procter]	any associated test.
17/09/1997 14:15:10	[Barry Procter]	[END OF REFERENCE 1905801]
17/09/1997 14:15:10	[Barry Procter]	Responded to call type T as Category 12 -Answered
17/09/1997 14:15:10	[Barry Procter]	The response was delivered on the system
18/09/1997 11:29:03	[Frank Fallon jun02]	In essence my original question was:
18/09/1997 11:29:03	[Frank Fallon jun02]	Is it acceptable to enter CAPS Link cryptographic key material remotely?
18/09/1997 11:29:03	[Frank Fallon jun02]	(The integrity of the key might be compromised).
18/09/1997 11:29:03	[Frank Fallon jun02]	
18/09/1997 11:29:03	[Frank Fallon jun02]	You have confirmed that at the VME end of the CAPS link the answer is no.
18/09/1997 11:29:03	[Frank Fallon jun02]	(The operating instructions define the procedure that must be followed).
18/09/1997 11:29:03	[Frank Fallon jun02]	
18/09/1997 11:29:03	[Frank Fallon jun02]	The PinICL can be cleared if the same operating instructions apply to the
18/09/1997 11:29:03	[Frank Fallon jun02]	Sequent end or if remote key entry to the Sequent is permitted. Is this

FUJ00103477

Ref	Summary	Opened	Last update	Customer	Product Group
Logged By		Closed	Status		Product At Fault
PC0005088	CAPS Link Crypto Key Mgmt:	15/07/1997 11:50:02	24/09/1997 15:59:41		Infrastructure
Fallon	restrict role to consol	24/09/1997 15:59:40	C		CAPS Link Crypto

18/09/1997 11:29:03	[Frank Fallon jun02]	information available yet?
18/09/1997 11:29:03	[Frank Fallon jun02]	
18/09/1997 11:29:05	[Frank Fallon jun02]	The Call record has been transferred to the Team: SecurityPolicy
24/09/1997 08:38:01	[Barry Procter]	Al, can you advise Frank of your ongoing discussions with Jeremy et al please.
24/09/1997 08:38:02	[Barry Procter]	The Call record has been transferred to the Team: TSC-Crypto-Dev
24/09/1997 09:09:40	[Roy Birkinshaw oct00]	The Call record has been assigned to the Team Member: Alan D'Alvarez
24/09/1997 10:47:19	Alan D'Alvarez	F} Response :
24/09/1997 10:47:19	Alan D'Alvarez	Ian, this PinICL has been addressed. The Operating Instruction have been
24/09/1997 10:47:19	Alan D'Alvarez	enhanced to clarify this further. Please ignore any reference to future
24/09/1997 10:47:19	Alan D'Alvarez	enhancements at Release 2 as this is subject to different issues that are
24/09/1997 10:47:19	Alan D'Alvarez	being progressed elsewhere. Please close this PinICL.
24/09/1997 10:47:19	Alan D'Alvarez	[END OF REFERENCE 1946368]
24/09/1997 10:47:19	Alan D'Alvarez	Responded to call type T as Category 12 -Answered
24/09/1997 10:47:19	Alan D'Alvarez	The response was delivered on the system
24/09/1997 13:53:07	[Frank Fallon jun02]	You mentioned 'Ian' and 'Release 2' in the response so I am unsure whether
24/09/1997 13:53:07	[Frank Fallon jun02]	you meant to send this reply. If so does this mean that remote key entry to
24/09/1997 13:53:07	[Frank Fallon jun02]	the Sequent is now permitted?
24/09/1997 13:53:08	[Frank Fallon jun02]	The Call record has been transferred to the Team: TSC-Crypto-Dev
24/09/1997 14:08:23	Alan D'Alvarez	F} Response :
24/09/1997 14:08:23	Alan D'Alvarez	Frank, I am not sure what happened on this PinICL, but somehow I must have
24/09/1997 14:08:23	Alan D'Alvarez	pasted the response to a different PinICL onto this one. The response should
24/09/1997 14:08:23	Alan D'Alvarez	have been:
24/09/1997 14:08:23	Alan D'Alvarez	It has been agreed with Jeremy Foulkes, PDA FSG, that the CAPS Key for the
24/09/1997 14:08:23	Alan D'Alvarez	Sequent can be loaded remotely. This PinICL can now be closed.
24/09/1997 14:08:23	Alan D'Alvarez	[END OF REFERENCE 1948018]
24/09/1997 14:08:23	Alan D'Alvarez	Responded to call type T as Category 12 -Answered

FUJ00103477

Ref	Summary	Opened	Last update	Customer	Product Group
Logged By		Closed	Status		Product At Fault
PC0005088	CAPS Link Crypto Key Mgmt: restrict role to consol	15/07/1997 11:50:02	24/09/1997 15:59:41		Infrastructure
Fallon		24/09/1997 15:59:40	C		CAPS Link Crypto

24/09/1997 14:08:23	Alan D'Alvarez	The response was delivered on the system
24/09/1997 14:59:40	[Frank Fallon jun02]	Thank you for your answer. This PinICL can be closed.
24/09/1997 14:59:40	[Frank Fallon jun02]	CALL PC0005088 closed: Category 12, Type T