FUJ00078389

Minutes of ICL/Utimaco Meeting - BRA01 05.11.98
Issue 0.1

Location: G45 Conference room, ICL BRA01 site in Bracknell
Date and Time: 11.00 on the 05th of November 1998
Attendees: Alan D'Alvarez (ICL Pathway), Paul McDermott (Utimaco), Peter McMahon (ICL Pathway), Philip Watkin (Utimaco)
Agenda:
1. Programme progress overview
1. KMS/SG VPN acceptance testing
   - Progress
   - Issues
   - Batch interface automation
   - Additional cryptware servers
1. SG VPN product acceptance testing update
1. Additional functionality
   - 'Soft start'
   - Extension of VPN to non gateway workstations
1. Any other business

Programme Progress Overview

Alan explained that the Treasury review had been positive with regard to the Programme and that they fully supported the revised Programme Plan which displayed a one month slippage for the start of NR2 Live Trial from the end of January to the end of February 1999. The Programme are aiming to hold the current NR2+ timescales of software development to be completed, including unit and link testing, by June 1999. This is the release that is currently targeted to include VPN.

KMS/SG VPN Acceptance Testing

Peter gave an overview of the MKS/SG VPN Acceptance Testing activity and presented details of the current issues. The Test references are derived from 'SG VPN Acceptance Criteria, TD/ARC/022, 3.0):

Test Status

Test	Status
1.1	Appears to be OK, but we can not currently prove that hardware randomness is being used. Can Utimaco provide information on how this can be proven ? (and are we in a similar situation as we are currently in proving the randomness of the number generated by the Comscire RNG ?)
1.2	Requires resolution to IR266, prior to being re-run
1.5	Appears to be OK, but in order to conclusively confirm that the session key has been changed, then we would require a LAN analyser and technical assistance from Michael Schmidt
1.6	Can not be run without the CRL Batch Interface (current estimate 15.11.98)
1.7	Require GUI version of RA application in order to generate a CRL in the correct format to work with VPN2.0. (This was supplied by Joe Basselier on the 03.11.98 but we are experiencing problems, Patrick Andries is investigating)
1.9	Whilst we have been supplied with details of the files that need to be backed up and the frequency of the backup, we are not in a position to run the test as the only way to prove the test is to rebuild the Cryptware Server and apply the backups. We are not in a position to rebuild the Cryptware Server - which raises the issue that I discussed with

FUJ00078389

	Jo last week, concerning how we rebuild the Cryptware Server in the event of a disaster as we have received no backup software and the means with which to apply it. Another interesting point raised is how we will recover from a disaster on the Cryptware Server when it is running in the secure environment in live usage.

Open Incidents raised with Utimaco

IR	Pr	Summary	Details/Progress
226	B	CRL list doesn't appear to work in VPN	Following failure of the initial SmartCards (see IR 214), Utimaco Belgium sent some test data for the VPN component, which consisted of several key files, and a CRL revoking one of the keys (Key 0016). When this CRL was introduced to VPN, it didn't appear to revoke the key, as encrypted communication could continue with it. This matter will be investigated further once we can successfully produce our own CRLs.
230	C	VPN logs an event when it receives a plaintext packet	Everytime a machine with the Utimaco VPN installed receives a plain IP packet, an entry is made to the NT event log. (actually if packets are received close together from the same source, they are summarised in one entry). When running on the unencrypted Post Office LAN, this will cause the log to fill up very rapidly. Events should only be logged if the plaintext packet is unexpected. i.e. The machine from which it is received is specified as an VPN partner which should be encrypting it's IP packets.
256	C	SGVPNSetKeyFile() returns success, when it fails.	When I try to introduce a key file to VPN, using an incorrect PIN, a SUCCESS code is returned, although the new key file has not been instantiated. This error has not yet been passed on to Utimaco, as I wish to ensure that the key file is of a valid format first (it is currently produced by a faulty RAB). 28/9/98 Michael Schmidt has indicated that the functionality is as agreed. The function merely updates the USWGSS.INI file with the new key file name, and sends a notification to the key service. It doesn't however check the integrity of the file. This IR should be kept open until it has been decided whether a validation check of the files contents is required.
259	D	Incorrect error message when certificate has expired.	When a VPN Key File has expired, the logon application VPNPIN shows the error message "Key is not valid as it is on the blacklist." is displayed. This is somewhat misleading as it implies the key is on the Certificate Revocation List.
266	B	Batch Interface should allow invocation from code.	The Acceptance Test criteria for the RAB batch interface specify that the interface should be callable from code. This is not currently the case, requiring the following manual steps: 1) Start up the RAB 2) Select Key Certification 3) Input the smart card

FUJ00078389

			4) Input the PIN 5) Press the START button to start processing a batch 6) Press the Close button 7) Exit the application.

Test 1.2 - IR266 (RA Batch Interface)
The current problems with the Batch Interface were described (i.e. that it currently requires a number of manual steps on each invocation). This issue was last discussed between Alex Robinson and Jo Basselier (Email dated 30.09.98) - in this mail item, two options to solving the problem were discussed and the mail item ended with Jo giving an overview of the 'best solution'. Since this mail item we have had no further dialogue on this problem due to other priorities and leave.

I was surprised to hear that Utimaco were already engineering a solution to this problem as we have received no further information concerning this problem. We therefore assume that it is the 'best solution' as described earlier.

ACTION1 - Jo and Alex to discuss solution to the Batch Interface issue, however in order to start this we need the specification of the current Utimaco solution to this problem

ACTION2 - Alan and Philip to decide whether this is part of the contract

Test 1.6
We require the CRL Batch Interface in order to run this test, current forecast 15.11.98 (dummy file only). It was mentioned that the CRL Batch Interface would be subject to the same considerations as the RA Batch Interface, however following subsequent discussions with Alex it transpires that the CRL Batch Interface is no more than additional data that is passed across the existing RA Batch Interface and as such any fix to the RA Batch Interface will be automatically propagated to the CRL Batch Interface.

Test 1.7 - IR226
Requires the CRL Batch Interface in order that a CRL of the correct format can be generated and used to test the VPN API. However, in order to run the test we have been supplied with a GUI RA Application that can generate CRL's - however, we are currently experiencing problems with this application.

COMM - Paul advised that this is escalated if not working by the end of 06.11.98

Test 1.9
This test can not run as it requires either an additional Cryptware Server (not available) or a mechanism to backup the Cryptware Server and rebuild from a CM Bill of Materials (not currently possible ?). This raised the more general issue concerning Maintenance of the Cryptware Server

FUJ00078389

ACTION3
Alan and Philip to agree Cryptware Server maintenance strategy

IR230
This was highlighted as a major problem which could cause the event logs on Gateway Counters to fill rapidly. Philip relayed Michael Schmidts comments that this was expected behaviour which would require a CP to change.

ACTION4 - Peter to investigate with Michael Schmidt and to escalate if it is proven that this will be a problem (N.B. this is related to the Phase 3 proposals concerning VPN encryption of the Post Office LAN)

IR256
Identified as a bug by Utimaco - A fix will be supplied if required

IR259
Currently under investigation by Utimaco

Additional Cryptware Servers
Alan explained that the order for additional Cryptware Servers would be released once Pathway have formally accepted the product. These will not be required until the end of March.

SG/VPN Product Acceptance Testing Update
Alan reported that analyses and development of the tools required to conduct acceptance testing of the SG VPN enhancements was underway. There was a delay n starting this due to the fact that Mark Jarosz was required to support the network re-design necessary to accommodate the introduction of SG VPN. This work needs to be implemented at NR2 and therefore took priority. The current target for completion of this testing is 30 November.

Additional Functionality
Philip distributed a document that has been prepared by Michael Schmidt and Tom Parker entitled 'SG VPN for Pathway - Phase 3 Extensions'. The document describes a proposal for two further extensions to VPN for Pathway, namely:

1. The capability to provide local LAN encryption
1. The capability to migrate from unencrypted to encrypted transmission

It was mentioned that feature 2 was to assist in the 2->2+ migration and was related to a new Pathway release (2.1). It was mentioned that the Crypto Development team were unaware of these proposals and that they would have to be impacted in relation to the release 2+ Design and Development Activity.

ACTION5 - Peter to distribute document and to provide a consolidated response to the proposal to include an impact on current 2+ design/development plans.

FUJ00078389

AOB

It was agreed that the current informal method of software handover would need to be formalised although the exact date and mechanisms were not agreed. Issues that ned to be resolved include:

1. Distinction between formal and Beta software handovers
1. Version control
1. Handover notes containing list of dependent software (such that patches are always installed in sequence)
1. Formalisation of handover route (software is currently received formally from Utimaco-UK and informally from Austria and Belgium). We need to establish a single point of delivery (Utimaco) and receipt (Pathway)

ACTION6 - Peter to grade Utimaco incidents in terms of High, Medium and Low as described in the VPN Acceptance criteria, the external reference field of the current IR form will be used to convey this information.