FUJ00077864

Exception plan for delivering KMS within current CSR+ timescales

1. Background

This paper follows the paper entitled 'Requirements for KMS at CSR+'. It supposes that Pathway accepts the KMS as critical for CSR+ acceptance, and summarises the various options that was open to Pathway to de-risk the delivery of KMS within Programme timescales. These timescales are themselves constrained by a number of outside influences:

- It is critical that ICL achieves go live of CSR+ on 17th April 2000
- This is required to bolster ICL's financial position with regard to flotation and the consequential benefits related to that

Currently KMS Development, including Module Test but not Link Test, is on track to the plan baselined in April. However, continuing increase in workload, coupled to a lack of contingency and budget allocation to cover all planned work have resulted in an increasing risk that the KMS will not be delivered within current Programme timescales.

Additionally, it has been accepted that there is no budget provision that could be allocated to 'shore up' the current development plan, and that the current aggressive downsizing of the team after July will cause 'Phase 2' deliveries to be slipped should any issues be found in the testing of the first Phase of delivery.

Therefore, this paper was commissioned to consider the options available to Pathway to effect the successful delivery of KMS for CSR+.

2. The way forward

2.1. Options

This section gives an overview of the options open to Pathway with regard to the delivery of KMS. Although it does not expand on any given option in any depth, it affords the reader an insight to the considerations undertaken before a decision was made with regard to the exception plan.

2.1.1 Maintain Current plan

Achievement against the current plan, as previously discussed, was displaying increasing workloads to meet milestone dates. It was becoming increasingly unlikely that the team could continue to maintain the increased effort in order to meet the scheduled delivery dates for code completion.

Additional to this the scope for Development Link Testing (DeLT) had been completed which resulted in a longer than anticipated DeLT phase. Pressure from the opposite end (BTC), along with emerging migration test requirements had caused the current plan to be non achievable without additional resource. This was further compounded by the extensive 'ramp down' of the team after code completion of the first Phase of delivery, adding significant risk to the support capability of the team whilst having to achieve equally aggressive delivery dates for the planned Phase 2 work.

Overall, even with additional resource, there was significant risk that the KMS would not have undergone sufficient testing in time to meet the current Programme Timescales. The table below demonstrates the timescales involved:

Timescale	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar
KMS Devt		Ph1		Ph2						
KMS DeLT Phase 1			Prt1		Prt2					

FUJ00077864

KMS DeLT Phase 2					Prt1	Prt2	Prt3			
TI					P1.1	P1.2	P2.2	P2.3		
System Test					P1.1	P1.2	P2.2	P2.3		
B&TC								P1.2	P2.2	P2.3

Even if Pathway were to accept the above timetable, considerable additional resource would be required to give effective support whilst completing the Phase 2 coding. This in itself may not be sufficient should any significant problem be found during the latter stages of testing.

2.1.2 De-scope: e.g. Go live with "phase 1"

Phase 1 of the KMS was never put together as a coherent set. Although it does provide functionality which can be tested, it does not represent functionality that could make up a release.

The advantages of this approach s that there will be less modules to both develop and test. Also, completion of the deliveries from Development to the test phases will be significantly sooner than the two Phase Strategy. However, to achieve this, some modules will need to be brought forward from the Phase 2 development work. There will be a further requirement for additional manual processes to be in place until such time as the Phase 2 functionality can be introduced.

It should also be noted that there will still be a requirement for additional resource to maintain the current quality processes.

2.1.3 Invoke the Contingency Plan

Early on in the KMS Project, it was established that it fell on the critical path for CSR+ delivery. As such, effort was expended to look at options for contingency should any major problems be encountered in the development cycle. This is detailed in TSC/CRY/006.

Although on the face of it this may be considered a viable option, it should be noted that the contingency plan was established to mitigate against 'disaster' as opposed to being a cost effective and viable long term solution. As such it has the following drawbacks:

1. Extra cost & resources required to achieve this.
2. These really need to start immediately as elements of the plan are sketchy.
3. Guarantees that we take our eye off achieving the current KMS plan; it is not possible to do both.
4. Contingency plan still subject to all the risks of the migration issues; indeed it is KMS that provides a migration mechanism (but still subject to risks), and without KMS, we have to achieve the migration manually.

2.1.4 Negotiate out contracted commitments

To de-scope the requirement for KMS, Pathway would need to negotiate 'lets' on the Cryptography requirement, i.e. KMS only supports the crypto solution. To make significant inroads into KMS complexity the following five requirements, specified in either the contract or contractually controlled documents, need to be negotiated out of CSR+:

- AP Signing
- VPN (with individually managed Keys)
- Crypto protection for the Quantum product
- Keys being generated using hardware random number generation (including FEKs)
- Public Key Certificates

History shows that the customer has been intransigent with regard to relaxing the 'contracted' security requirement. Although the removal of BPS would give credence to a review of the

FUJ00077864

security solution, in particular the use of cryptography, the timescales in which CSR+ is operating make reliance on such activity too high a risk.

2.1.5 Spend contingency plan / other money on current plan

The contingency plan is not cheap and would need to be effected in addition to current work on the KMA (holding the KMA team on longer to complete this in the long run). The extra costs of doing this could be spent on bolstering the current plan and de-risking the Development link Test and KMS System Test. However, this would require the employment of additional resource, who would require a working environment. This would be difficult to achieve in the current climate at Bracknell.

2.2. The way ahead

Steer from the meeting with Terry Austin held 9th June

At the meeting held on 9th June [att. Terry Austin, Pete Jeram, Alan D'Alvarez, Chris Humphries, Gill Jackson] the above options were considered with the following results:

> 2.1 Maintain current plan - considered too high a risk in the light of increasing work over that planned and the resulting pressure on the teams ability to meet planned dates
>
> 2.2 De-scope : Go live with 'Phase 1' – Considered a viable way forward with minimal overall impact on cost
>
> 2.3 Invoke the contingency plan – Considered to have a fairly high risk factor which would incur additional nugatory cost
>
> 2.4 Negotiate out contracted commitments – Considered too high risk due to past customer intransigence
>
> 2.5 Spend contingency plan / other money on current plan – No budget available to fund this option

The clear steer from the meeting was to pursue option 2.2 and to scope whether this was a viable option within the current budgeted head count. Completion of Phase 2 would need to be scheduled for introduction in a future release supported by a budget CP.

3. Exception plan for de-scoping the content of KMS at CSR+

Accepting the above steer, this exception plan documents the deliverables required to effect a functional KMS for CSR+. It also considers the components being de-scoped from this release, along with the impacts and associated risks.

3.1 Phase 1+ KMS

The Drivers for cryptography at CSR+ are:

- Crypto is required to support the business requirements of APS & L&G
- Crypto is required to support the infrastructure requirements of VPN & FEKs
- Certification is required

The events when the KMS functionality are required:

1. Data Centre Migration to CSR+
2. Roll-out of CSR+ Counters
3. Counter Migration to CSR+
4. Counter Swap out
5. Key Compromise

FUJ00077864

6. Key Change

The phase 1 KMS devt to KMS DeLT drop targeted for July delivers the majority of code for this functionality. However, there are a number of deliveries, currently scheduled for Phase 2, which contain functionality required to manage the above events.

The phase 2 KMS drop contains the following modules:

- Manual New Key
- Key Importer
- Capu checker
- Garbage collector
- Integrity Checker
- Revoker

The above functionality can be achieved if we add to phase 1 the following three components currently scheduled as part of the Phase 2 delivery:

- Manual New Key Required to support manual channel for SI and KMA
- Key Importer Required to initialise KMA and for migration of SI

The following table annotates the events will be satisfied; firstly within the original scheduled release, and then the proposed additionalmodules to be brought forward from Phase 2:

	Event	Phase 1	Phase 2	Phase 1+	Phase 1+ Component
1	Data Centre Migration to CSR+	X	Y	Y	Man New Key/Key Importer
2	Roll-out of CSR+ Counters	X	Y	Y	Man New Key/Key Importer
3	Counter Migration to CSR+	Y	-	Y	
4	Counter Swap out	Y	-	Y	
5	Key Compromise	X	Y	Y	Revoker
6	Key Change	Y	-	Y	

So how would we live in a phase 1+ world without:

1. Capu checker Work round this with Tivoli type scripts; developed after July
2. Garbage collector Defer to later release (sufficient EMC disc space for 2 years)
3. Integrity Checker Either drop (and accept the risk involved) or slot in later

3.2 Additional actions to reduce KMS content for CSR+

Further actions to reduce KMS content in phase 1+:

The requirement for early VPN (i.e. prior to introduction of KMS) means that an off line process is required to generate the initial set of VPN keys for the campus NVPN (Private VPN Keys for Campus VPN Servers) and FVPN/EVPN (Global keys for Post Offices).

This will be performed using the KMS CA Workstation (i.e. a Utimaco Cryptware server) using the standard Utimaco GUI interfaces. By providing secure access for an additional CAW role, the management of these keys can be kept manual for KMS phase 1+. Live support for these platforms by KMS would be restricted to CRL distribution. Design effort is required (post July) to document the process for management of these including key compromise situations. The latter would require testing, but there is minimal KMS specific code.

The removal of BPS means that 3 protection domains can be removed, and consequently implementation of any remaining incomplete Phase 2 KMA deliveries can be reduced, for example:

3. CAPS No support for CAPS keys in Key Importer and Manual New Key

FUJ00077864

4. PA No support for migration of PA keys in Key Importer
5. CMS No special case code (i.e. data driven) but no need to test this feature.

[Note that there is a potential requirement for PA key to sign AP acknowledgements, but this proposal is not within the scope of Phase 1+. Any such move to introduce this for CSR+ would need to be covered by a CP]

Pathway confirmed that KMS at CSR+ should only interface with counter facing Keys; which will significantly reduce the test requirements for the KMS at CSR+ on the following platforms:

1. FTMS links for POCL TIP
2. FTMS links for Archive Server
3. FTMS links for HAPS disaster standby system
4. FTMS links for POCL TIP disaster standby system
5. FTMS links for AP Clients
6. Rambuttan reminder mechanism for Key Manager

This means that for all except the last item, these would (continue to) be supported by an NR2 style offline Manual Key Service operation. There is a residual issue concerning the requirement for Public Key Certificates for these platforms which is being investigated by Dave Johns.

3.3 Implications on Testing phases:

1. Review of risks, identify an immediate release to other Pathway DU test streams of the CSR+ Crypto product on the supported platforms (i.e. FTMS platforms would stay with NR2 Crypto)
2. Single drop strategy into DeLT means that KMS DeLT can proceed without use of testing stubs, effectively being a pre-PIT systems test but without fully representative platform builds
3. By going for a single drop of KMS, we can eliminate some aspects of the work – in particular re-work building different environments as new code arrives
4. Some code may be released at an earlier stage in quality cycle (e.g. pre code inspection / module test), providing main paths are unit tested, further updates could be incorporated in bug fix handovers as a calculated risk
5. Testing time is only really reduced by removing functionality from product. Phase 1+ goes some way on this, but need to re-review in case further de-scoping is possible to reduce risk

3.4 Follow on KMS release:

This de-scoped release of KMS provides a viable system for managing Crypto keys for the initial period, but an update to KMS will be required within 2 years to address the shortfall

1. The FTMS software will need validating on the new style crypto to address shortfall such as Certification
2. To provide a manageable way of supporting the target AP Client population (300?)
3. To reduce the support load on the Crypto team by removing support for NR2 code
4. To reduce the ongoing Managed Key Service workload and skills necessary to do it.
5. To automate the CAPU checking mechanism and reduce manual load
6. To provide garbage collection for KMA database
7. To manage all VPN keys, and remove manual (potentially error prone) mechanisms around Key changing and revocation.
8. To rectify any shortfall and manual work-arounds around Key compromise and revocation.
9. To support additional Protection Domains as they emerge (e.g. signed AP Acknowledgements).

Appendix A shows the revised KMS Development project plan to support the Exception Plan.

FUJ00077864

4 SDU Test Strategy to Support Delivery of Phase 1+

Appendix B shows the high level SDU test project plan supporting the Phase 1+ strategy. Contained within this are three delivery streams into Technical Integration, after which formal System testing can take place. During each delivery stream, there will be an element of joint Link Test/System Test activity, much of which will be done prior to the product being handed over to PVCS. This will allow the teams to stabilise the release prior to the application being entered into a formal baseline which would bring with it the extensive overheads associated with introducing fixes on. At this stage, the team will utilise an access database to track and record progress with regard to any bugs, fixes and issues.

Each 'Baseline' will have a content description, the target environments for that baseline and availability dates from Technical Integration. There will also be a dependency list which, if missed, will slip dates. Risks are catalogued at the back of this paper.

4.1 Baselines

4.1.1 Baseline 1

This baseline will consist of the redelivery of Crypto code which will be supported by KMS. This element is seen as invasive to the business functionality and therefore has been targeted for introduction to the test arena as soon a practicable. Once business applications have confirmed that they are ale to sign and verify messages with the revised Crypto code, there will be minimal requirement for regression testing with regard to the business applications on future baselines.

Content:
- Crypto functionality, AP and SI - module tested
- Stubs for the supply of Crypto Keys
- Siemens Metering protection (to be confirmed)
- Will not support migration (will require handcrafting for CSR - CSR+ building)
- Will not support VPN (VPN will be tested utilising Global Key at this stage)
- POLO will be retained at CSR (not CSR+ product)
- will not support CSR+ autoconfig.

Target Environments:
- Security Delivery Unit System Test - Crypto and VPN (Global Key)
- POCL Products Delivery Unit
- B&TC

Availability from Technical Integration:
- System Test - 13th August
- B&TC - 15th October

Dependencies/Assumptions:
- System Test requires environment (both space and test rig) to be built and operational by 30th July
- System Test will require KMS rig, VPN rig and Secure Builds rig (to be defined)
- Technical Integration will take 5 days to assimilate handover into a baseline

4.1.2 Baseline 2

This will consist of the first delivery of KMS functionality to support the revised Crypto code. The prime purpose of this baseline is to pipe clean the formal build process and to start the SDU System Testing of KMS. Hence, there is no target audience for this baseline outside of the SDU or Technical Integration. There will be a link test phase along with a joint system test pre validation exercise prior to hand over to PVCS.

FUJ00077864

Content:
- Phase 1 KMS (with the two additional modules)

Target Environments:
- Security Delivery Unit System Test
- Technical Integration

Availability:
- Into Technical Integration - 24 August
- Into SDU System Test 7 September

Dependencies/Assumptions:
- Link Test requires delivery of equipment by 30th June
- Will require Technical Integration resource assigned to the Crypto Team early in July
- Technical Integration will take 10 days to assimilate handover into a baseline
- Will require CM/Technical Integration to maintain a dual baseline

4.1.3 Baseline 3

This will consist of the first delivery of KMS functionality to all units in Pathway.

Content:
- Phase 1 KMS (with the two additional modules)
- Test Keys
- Supports migration

Target Environments:
- Security Delivery Unit System Test
- Internal Infrastructure Delivery Unit System Test
- Technical Infrastructure System Test
- B&TC
- Live

Availability:
- From Technical Integration for System Test - 15 October
- For B&TC - 26 November

Dependencies/Assumptions:
- Migration dependencies for Data Feeds, Autoconfig, Counter Processes and System Management are met
- The KMS specific platforms will be required to utilise this baseline
- Will require other Delivery Units to either have a KMA to test Key interfaces, or to utilise/develop stubs
- May require CM/Technical Integration to maintain multiple baselines

5 Risks

Going live with Phase 1 of the KMS delivery, along with selected other modules, presents a number of risks. These are catalogued in more detail in the risk paper. The Crypto team have been working to the production of KMS to an established baseline and it must be recognised that a change in focus and direction in itself presents risk.

FUJ00077864

The above strategy for a way forward, although sound in concept, requires technical validation. Bringing the various modules forward to create a manageable cohesive release will necessitate the cutting of quality processes for these modules to achieve the revised timescales. Additionally, the missing functionality will necessitate the adoption of manual workarounds, which in turn will require resource to develop and test.

It is certain that issues related to migration, and other factors such as CPs and design creep found to be necessary (vs creep that can be rejected) threaten the achievement of successful delivery.

The following table catalogues those risks from the SDU risk database pertinent to this exception plan:

RD Ref	Description of Risk	Proba-bility	Impact	Risk Factor	Mitigation	Mtgtn Impact
R02	Migration Complexity causes conflicts between products causing additional work/rework impacting delivery date and costs	**P**	10	TBA	1) Focus Resource on Pathway migration issues 2) Employ Full-time Migration TDA	P) P I) - 2
R37	Inadequate budget, will compromise delivery and support strength with potential for delays when encountering technical problems downstream	8	10	80	1) Assign additional resource for initial support at early stage of testing. 2) Manage risk of potential issues at the latter part of testing through constant review of resource requirements	P) - 4 I) - 3
R71	Replan, condensed timescales & budget constraints absorb all contingency plus ability to handle further CPs, change or resource hits	8	9	72	1) All further change / resource/impacts must be resisted 2) Budget for contingency	P) - 3 I) - 3
R58	Reduced support capability for KMS in System Test will delay PinICL fixes	8	9	72	1) Retain additional support resource	P) - 5 I) - 5
R41	Build availability - lack of, will slow down DeLT, SDU Sys Test & B&TC	8	9	72	1) Obtain resourced TI plan to link with SDU plan	P) - 4 I) - 2
R59	MKS to address KMA 1+, shortfall unknown, leading to delays in production of testkeys, and manual processes	8	8	64	1) Additional design effort required to scope work	P) - 6 I) - 2
R60	Reduced support capability for KMS in B&TC will delay PinICL resolution	8	7	56	See R37	
R44	CM / PIT capability to support multiple baselines is critical to downstream testing. Risk of large delays whilst test streams recover from wrong baselines	7	8	56	1) Document and agree process for managing multiple baselines with CM/PIT	P) - 5 I) - 0
R53	Disappearing Skill Base; with potential for delays caused when encountering technical problems downstream	8	8	64	1) Create time (hence cost) for skills transfer into core support team	P) - 5 I) - 5
R61	Reducing scope of KMA MTSs causes extra bugs in DeLT, and could delay completion of DeLT / reduce quality of output	9	8	72	1)Run KMA pre-DeLT integration 2)Additional development support for DeLT 3)Run remaining MTS tests during DeLT	P) - 4 I) - 3
R36	Inadequate or late DeLT kit threatens DeLT ability to complete and hence could give rise to delays downstream	6	8	48	Progress DeLT KIT orders immediately	P) - 2 I) - 0
R62	Reduced support capability for KMS in Live Service, could delay PinICL fixes	6	7	42	Monitor support requirement through test phase. Assess and procure appropriate resource	P) - 5 I) - 4

FUJ00077864

RD Ref	Description of Risk	Proba-bility	Impact	Risk Factor	Mitigation	Mtgtn Impact
R48	DeLT & System Test time-scales condensed & overlapped	6	7	42	Budget required for parallel resources	P) - 5 I) - 6
R32	Lack of space for Dev. Infrastructure and DeLT staff, threatens DeLT ability to complete and hence could give rise to delays downstream	10	4	40	1)Issue escalated through Pathway Management route - Alan D'Alvarez	
R47	Long PIT time-scales, could threaten delivery dates. (Plans assume builds available within 5 days)	8	8	64	1. PIT staff to participate in KMS build process 2. Production of resourced PIT plan to dovetail into SDU plan	P) - 5 I) - 5
R21	Requirements Document [REQ] still not baselined; risk of further change	4	8	32	1. Baseline as rapidly as possible 2. Allow additional capacity in plan for this	P) - 3 I) - 4
R73	Inadequate security in L&G test envt & processes requires additional cost	4	8	32	1. Review proposed test plans for L&G	
R56	External interfaces with other Pathway infrastructure areas not committed threatening stability of design; possible rework and delay	7	8	56	1. Separate documents covering agreements with other DUs 2. Design team to monitor other units for design specs and delivery dates.	P) - 3 I) - 1
R64	Bringing forward Ph2 components into Ph1 reduces quality of other components with potential delays in subsequent stages eg DeLT, & SDU System Test	8	7	56	1. Run KMA pre-DeLT integration 2. Additional development support for DeLT	P) - 4 I) - 6
R68	Cutting KMA code inspections causes extra bugs in DeLT; with potential risk of delays downstream	8	7	56	1. Run KMA pre-DeLT integration 2. Additional development support for DeLT	P) - 4 I) - 6
R40	Design creep, could threaten delivery dates	10	5	50	Freeze design	P) - 10 I) + 3
R51	External dependencies on KMS not declared yet (eg stubs, test keys etc), and resourcing such requests will delay deliveries and support	6	5	30	Additional resource to cover risk	P) - 0 I) - 4
R72	Other risks in risk register underestimated causing additional hits if occurring	5	5	25		
R1 (ST)	System test environment not yet allocated	8	10	80	Allocate secure test cell to SDU and equip with additional test equipment for KMS by 30 June	P) - 7 I) - 9

Note - Where the probability is assessed as 'P', this dictates that the risk is outside of SDU control and would need to be assessed at a higher level within Pathway with due cognisance to all available information.

6. Costs

6.1 Cost of exception plan

The main driver behind the exception plan was to deliver KMS within the current Programme timescales and within the current KMS Budget. Costs are measured as headcount resourcing levels only.

The following table details the KMS Development and System test team headcount profile to support the exception plan. The previous headcount profile is illustrated to show how resource is being re-allocated to achieve the Phase 1+ baseline and to mitigate against some risks.

FUJ00077864

Team	Apr '99	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan '00	Feb	Mar	Total
KMS Dev Budget	50	50	50	50	30	26	25	23	20	20	20	20	384
KMS Dev Forecast	**45**	**47**	**49**	**48**	**49**	**36**	**29**	**24**	**21**	**12**	**12**	**12**	**384**
Under/OverSpend	-5	-3	-1	-2	19	10	4	1	1	-8	-8	-8	0
System Test Budget													
System Test Forecast													
Under/Over Spend													

[Note : the System Test headcount profile will also be responsible for validating VPN and the Secure Builds]

6.2 Cost of Risk Mitigation

The table below assesses the cost (in additional headcount profiled across the timeline) required to mitigate the risks identified in section 5. Unless budget is released to invoke mitigating actions, these will not be factored into the exception plan.

Risk	Apr '99	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan '00	Feb	Mar	Total
R2					1	1	1	1	1	2	2	2	11
R71					2	3	2	2	1	1	1	1	13
R58						4	4	4					12
R41				2	2	2	2						8
R59					1	1	1	1	1	1	1	1	8
R60									4	4	4	4	16
R48					4	4	4	4	4				20
R73					1	1	1						3
R56					**1**	**1**	**1**	**1**					**4**
R64					**1**	**1**	**1**						**3**
R68					**1**	**1**	**1**						**3**
R51					**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**8**

7 Summary

On approval of the exception plan a supporting Project Plan will be lodged in the Programme Office to replace the existing KMS plan. Pathway will assess the success of delivery against the exception plan and a CP will be raised for the introduction of de-scoped functionality at a later release.