# Requirements for Key Management

Reference: RS/REQ/009

Issue: 2.0 APPROVED

Date: 20th April 1999

Abstract: This document examines the management of keys within Pathway; it analyses how they were managed in Release 1c, and defines the requirements for key management in NR2+.

Approver: Barry Procter

Signature & Date:

***This is a controlled document****. This issue is definitive if it is the latest, which has gained the approver's signature.*

*Check with the document controller (below) that this is the latest issue.* ***An out-of-date issue or a non-approved issue is not definitive****.*

*Controlled by: Tom Parker* *Location: HOM99* *Phone:* GRO

*Electronic repository: Pathway Library*

Distribution:

| | | | |
|---|---|---|---|
| BRA01 | Rob Arthan | FEL01 | David Jones |
| BRA01 | Roy Birkinshaw | BRA01 | Tom Parker |
| IRE11 | Vince Cochrane | FEL01 | Barry Procter |
| FEL01 | Alan D'Alvarez | BRA01 | Alex Robinson |
| FEL01 | John Dicks | FEL01 | Glenn Stephens |
| FEL01 | Stephen Doyle | BRA01 | Chris Sundt |
| BRA01 | Belinda Fairthorne | FEL01 | Peter Wiles |
| BRA01 | Peter Harrison | | |
| FEL01 | Mark Jarosz | | |
| FEL01 | Peter Jeram | FEL01 | Pathway Library |
| BRA01 | David Johns | | |

# DOCUMENT CONTROL

## Changes in Version 0.6

Comments received on the previous version have been responded to.

Terminology definitions have been expanded to clarify the meaning of entries in individual key tables.

The section on Riposte keys has been expanded.

Requirements on key algorithms, sizes and expiry have been added.

Requirements arising from the Pathway Access Control Policy [ACCPOL] have been added.

The "Social System" section has been greatly extended and brought up to date.

## Changes in Version 0.7

Comments received on the previous version have been responded to.

Although internal keys CK and KI are described for completeness, no specific requirements are identified for them, since these are merely a part of the anticipated solution, and may be replaced by alternative solutions (though this is unlikely).

The key tables have been updated with new information, and a summary table of what keys are supported where has been added as an Appendix.

The requirements for CHAP keys now mention the possibility of VPN as a substitute for at least some post offices.

Key Custodian and Key Handler perspectives have been added.

## Changes in Version 0.8

Version 0.8 included minor amendments in response to informal comments, and was the input document to the formal review procedure.

## Changes in Version 1

Includes amendments resulting from the formal review procedure. This version is intended to be the first approved Version.

## Changes in Version 2

In outline, these are:

1. The scope is more precisely defined, focusing on functional business requirements only.
2. VPN related requirements have been added, along with an outline description of the VPN functions being supported. Superseded CHAP requirements have been taken out.
3. AP signed messages no longer need to retain their signatures beyond the campus agent that receives them from the post offices. The requirements have been changed to reflect this.
4. There is no requirement to sign data transmitted from AP clients. The requirements have been changed to reflect this.
5. An additional physical protection requirement for CAPR has been added.
6. The requirements for CAPU handling have been clarified, maximum verification frequency is still to be decided.
7. The POK requirements now describe current thinking on usage of POK.

8. A description of the new TK key has been added, though since this is an internal key it gives rise to no additional business requirements.
9. There are no CA keys in use in NR2. Requirements relating to this have been deleted.
10. The description of the KMA key's usage has been changed to reflect its use now via the mirrored KMC server database.
11. The generic requirements originally described as an extract from [CRYPARCH] have been more loosely related to [CRYPARCH].
12. Requirements relating to the social system view of system management have been revised to reflect that use of Riposte instead of Tivoli for key material.
13. The network management requirements have been significantly changed – they were mostly related to CHAP change synchronisation, which is no longer an issue. However new requirements arise in relation to VPN.
14. A new requirement asking for the management link to the KMC server to have high security has been added.
15. Changes reflecting the need for the Pathway Key Manager to delay revocation based on a business risk decision have been made.
16. A migration requirement relating to VPN has been added – "no manual intervention".
17. CA failure recovery requirements have been clarified.
18. A requirement that routine key change procedures should be simple and well defined for the postmaster has been added.
19. A requirement that technical support must not be prevented from doing their job, while at the same time live key material should not be compromised has been added.
20. Requirements stemming from the perspective of the post office trainee (in training mode) have been added.
21. A variety of textual changes have been made to correct errors and bring the document in line with latest design thinking.

## Changes in Version 3

1. Changes responding to comments received.
2. New section on L&G (now Siemens Metering) key material
3. VPN split off into a section of its own.

## Changes in Version 4

1. All requirements are now numbered, with explanatory text provided in the Organisation part of the Introduction to describe the numbering scheme.
2. As part of the review occasioned by the numbering operation, repetition of requirement statements has been removed as far as has been practicable. Repeated general requirement statements against each specific key type for NR2+ have been replaced with a single statement for that key type along the lines of: "X must be supported in a manner that meets all applicable general requirements".
3. Requirements relating to CA keys in NR2 (intended to have been removed in the previous version, but left in error) have been removed. There are no certificates and no CA keys in use in NR2. Current thinking for NR2+ CAPUs is to deliver a brand new set as a part of the migration operation and then

immediately perform an integrity check using the standard NR2+ CAPU checking mechanism. A requirement for this integrity check to be made before the new CA keys can be used has been added.

4. There are section number changes that have resulted from the insertion of new ones.
5. A number of minor wording corrections have been made.
6. There is an additional change forecast, relating to Belfast home working.
7. Outstanding issues are now all collected together at the end of Changes Forecast.
8. The requirement for VPN keys to be unique is now only in relation to post offices (campus servers can share a private VPN key).
9. The requirement that AP application code must not need to be changed, which is a hangover from when we were planning to support AP signing in NR2, has been removed.
10. A new Section 2.17 has been added, spelling out requirements relating to additional FTMS protection domains, with specific requirements to support keys for Archive Servers in NR2.
11. An anticipated frequency of checking CAPUs has been added to Section 2.10.4.
12. The different stages in the key management process for AP, FEK, FTMS and POCL TIP keys have been described in outline, consistent with similar descriptions for other key types.
13. The Requirement in Section 2.15.5 that each AP client has a different FTMS key is wrong and has been removed. A different key is required only in the case of symmetric encryption keys and for clients that themselves are signing things. Neither of these apply in NR2+; only Pathway sign data on the way out to clients, so no client can compromise another one as a result of having poor security. There is a corresponding change to the FTMS key table (only one key needed instead of one for each client).
14. A requirement to support seasonal and permanent closures of post offices has been added as Section 3.1.4.
15. The requirement in Section 3.4 has been generalised so that there is no longer any implication that a Key Custodian must have access to the KMA's logs.
16. In Section 5.1.1 the text no longer implies that if a CD-ROM is supported on a platform, the key management system must provide key material on a CD-ROM.
17. In Section 5.4.1 a requirement to preserve the security of broken CAWs has been added.
18. In Section 5.10.1 a requirement to be able to support post office PMMC recovery when the connection to the central campuses is down or the KMA is not available, has been added.
19. The description of TK in Section 2.14 has been modified to reflect the extension of the use of the term to manually transmitted red keys to non-post office destinations.
20. A requirement has been added to Section covering the revocation of AP and VPN keys of post offices that close, and the removal of the post office as a destination for key issue from the KMA database
21. L&G is now referred to as Siemens Metering, and supporting the statements in the contractual statements document associated requirements has been added as an explicit requirement.
22. There may be changes to the way the Siemens Metering DLLKA is handled, so the wording of the requirement relating to the split between DLLKA and DLLKB has been generalised to accommodate this possible change.
23. The requirement for post offices to report back on keys that have been installed, and for the KMC react to late installation notifications has been added to Section 5.1.1.

24. Some requirements were present against the KMA key, despite the fact that non-business key requirements have been declared out of scope. They have now been removed.
25. Section 3.1.3 on Routine Key Expiry has been merged into the section preceding it, as there was some duplication of requirement.
26. The requirement in Section 4.3, that access to campus LANs is confined to being through VPN servers, is out of scope and has been removed.
27. In view of the new requirement that recovery from lost PMMCs must be possible if the communications link or the KMC is down, requirements on KMC resilience for this purpose have been removed.

## Changes in Version 5

1. The Autoconfig signing servers are now explicitly mentioned in the descriptive part of Section 2.7 on SI keys. There are no requirement changes.
2. Bullet 3 of Section 5.1.1 contained a requirement for warning reports on automated key changes. Alex had concerns about the value of these, with which I agree. The bullet (bullet 3) has been changed to: "For keys whose management is not fully automatic, the system must prompt a month in advance of key change being due **(Req't: G50)**, and then, until the key change is confirmed complete, again on the day the key change is due **(Req't: G51)** and daily thereafter **(Req't: G52"** in response to Alex's concern that a report of an imminent automatic key change. There is a matching change in Section 5.14.1.

   So **Req'ts G50**, **G51** and **G52** in Section 5.1.1 have changed slightly - they except fully automated keys.
3. The wording of the requirement to check CAPU values has been changed to reflect the requirement rather than a specific solution (which was different from the one being implemented!).
4. Errors in the text describing TK have been removed. There is no requirement change.
5. The text describing Siemens Metering values has been cleared of minor errors.
6. The GDK filestore protection requirement no specifies which crypto key has to be used to encrypt it.
7. Some additional issues have been added to the box at the end of "Changes Forecast".

## Changes in Version 6

1. Two of the VPN requirements had not been annotated with requirement numbers. The annotations have now been added (**Req'ts S104** and **S105**). These requirement numbers had been provisionally earmarked for requirements related to VPN policy files, but it has now been agreed that policy files are not a KM responsibility.
2. At the suggestion of Peter Robinson, a mention is made of VPN PIN values, though this has generated no additional requirements. See Section 2.4.
3. Many of the issues identified in Changes Forecast have been resolved. The resolutions are reflected in the relevant Version 6 changes listed below.
4. A requirement **G114** has been added to ask for duplicate floppies to be made, avoiding single point of failure problems.

5. Requirement **S36** in Section 2.10.4 has been deleted, permitting Tivoli to deliver CAPUs, provided that they have been verified before use. This has also caused a subtle change to **S37**.
6. On the basis that it has been agreed that the VPN policy file is outside the scope of the KM system, the associated issue has been removed.
7. A new requirement to be able to split DLLKA/B in a different way for a post office, following a possible key compromise, has been added (**S106**).
8. Text explaining the way in which requirement numbering is affected by changes in requirements has been added to Section 0.7
9. The requirements for key uniqueness when adding new FTMS links have been clarified - see **S46**, **S47** and **S48** in Section 2.17.2
10. Requirement **S96** demanded the ability to recover not only when the post office is on line, but also when the KMA is not available. The latter is not a requirement and has been removed.
11. An index of requirements has been added.
12. There have been a number of minor wording changes responding to comments.

### Changes in Formal Issue 2.0

In this issue we start to use (for the first time!) the correct formal numbering scheme. Since the last formally approved version was Issue 1, we now call this version Issue 2.0. The changes below were made following comments received at a formal inspection of Version 6, held on the 31st of March 1999. The requirements identified in the list of changes that follows below follow the numbering used in Version 6. Of those requirements that remain, many have now been renumbered.

1. The current terminology for release versions is now used throughout (viz: NR2 and NR2+).
2. The scope has been refined to focus on NR2+ requirements. NR2 requirements have been left in as historical information, but are no longer numbered.
3. A new requirement that live confidential keys must not be used in testing environments has been added.
4. Requirement **G71** now gives outage times and references the relevant contractual document.
5. The locations of Help Desks are now correctly identified in Section 4.7.
6. In Section 5.1.2, requirement **G62** has been reworded to focus on the underlying rationale for the requirement, and requirement **G63** has been made more precise.
7. The title of the POCL TIP Section has been corrected - it now reads “POCL TIP Link”.
8. The type of extensibility in requirement **S50** (relating to support for key material for future applications) has been refined to be able to be “via incremental development”.
9. Requirement numberings have been reset to contiguous values, and a new category type of P for procedural has been added. As many of the old numbers as possible have been retained.
10. The nature of permitted channel split has been clarified in Requirement **G63**.
11. Some other minor clarifications have been made.
12. Requirement **S37** for integrity verification of dynamically installed CAPU values has been slightly relaxed to fit with what is possible.

13. The requirement over the roles involved in key management administrative processes has been expanded into three different requirements. Their technical, as opposed to procedural, nature has been emphasised. See Section 4.4.
14. Requirement **G3** (that Red Pike keys should be 64 bits long) has been removed - it is a fact of life not a requirement.
15. Two new requirements relating to additional FTMS links have been added in Section 2.17.2: one to explicitly bring out the need for a signing key to be different if it is held at a different physical site, the other to require control over acceptance of private keys used for signing backup copies of live material.
16. Implications of perfect synchronisation between the KMC's and a post office's view of which key changes have occurred at the post office have been removed from requirements **G9** and **G50**.
17. The Siemens Metering requirement not to hold both DLLKA and DLLKB on a post office PC's filestore has been qualified to permit this if one of them is encrypted. Other minor wording changes have been made to bring these requirements in line with the contractually agreed [STAT].

## Changes Forecast

The changes identified below, if needed, will be made under formal change control procedures.

1. Requirements for management of key material for the protection of links from home working support staff in Belfast will be added when proposals in this area have been accepted and stabilised.

## Document history

| Issue | Date | Reason |
|---|---|---|
| 0.1 | 1.10.97 | Draft for internal comment |
| 0.2 | 21.10.97 | Draft for internal comment |
| 0.3 | 22.10.97 | Draft for Distribution |
| 0.4 | 17.11.97 | Re-drafted to incorporate comments and re-structure |
| 0.5 | 10.05.99 | Comments included for wider circulation |
| 0.6 | 3.2.98 | Document taken over by Tom Parker. Comments received on Version 0.5 included. Further requirement refinements added as described in "Changes in this version" above . |
| 0.7 | 3.3.98 | Changes as described above |
| 0.8 | March 1998 | Changes as described above |
| 1 | 8.5.98 | First approved version |
| 2 | 30.9.98 | This unapproved version, brought up to date with current design ideas |
| 3 | 16.11.98 | Responding to comment, now needs re-approving. |
| 4 | 18.12.98 | Responding to further comment and new requirements. Many requirement statements restructured as part of the introduction of requirement numbering – needs re-approving. |
| 5 | 22.02.99 | Various changes responding to comments and events. |
| 6 | 18.03.99 | Various changes in response to formal comments prior to inspcetion. |
| Issue 2.0 | 07.04.99 | For Approval - updated to reflect further comments received in formal inspection. |

## Cross References

| | Title | Reference | Issue | Date |
|---|---|---|---|---|
| [SFS] | Security Functional Specification | RS/FSP/0001 | 3.4 | August 98 |
| [TED] | Technical Environment Definition | TD/ARC/0001 | 3.2 | t.b.s. |
| [SADD] | System Architecture Design Document- | CR/FSP/0004 | 5.1 | t.b.s. |
| [POKM] | Post Office Key Management | RS/DES/021 | 8 | t.b.s. |
| [SEM] | Security Event Management Requirements - | RS/REQ/004 | 0.2 | 01/10/97 |
| [HLD] | Key Management High Level Design | TSC/CRY/010 | 2.0 | November 1998 |
| [ACCPOL] | Access Control Policy | RS/POL/0003 | 2.21 | November 1998 |
| [CRYPARCH] | Cryptography Architecture | SD/DOC/002 | 0.2 | May 1998 |

| | | | | |
|---|---|---|---|---|
| [STAT] | Statements on Security Objectives and Methods for the Protection of Siemens Metering Code and Data | RS/FSP/003 | 4 | March 1999 |
| [G10] | Schedule G10 of the main contract | | | |

## Abbreviations

| | |
|---|---|
| AP | Automated Payment |
| APPR | AP Private Key |
| APPU | AP Public Key |
| BA | Benefits Agency |
| CA | Certification Authority |
| CAPR | CA Private Key |
| CAPU | CA Public Key |
| CAW | Certification Authority Workstation |
| CAPS | Customer Accounting and Payment Strategy |
| CHAP | Challenge Handshake Authentication Protocol |
| CK | Communications Key |
| CMS | Card Management System |
| DLL | Dynamic Linked Library |
| DLLEK | The Siemens Metering DLL enabling key |
| DLLKA | A key component which, together with DLLKB is used to form DLLEK |
| DLLKB | A key component which, together with DLLKA is used to form DLLEK |
| DSA | Digital Signature Algorithm |
| FEK | Filestore Encryption Key |
| FTP | File Transfer Protocol |
| GDK | Global Distribution Key, the key under which Siemens Metering code is to be encrypted in delivery |
| HAPS | Host Automated Payment System |
| ISDN | Integrated Services Digital Network |
| KI | Key Issue |
| KIPR | KI Private Key |
| KIPU | KI Public Key |
| KM | Key Management |
| KMA | Key Management Application |
| KMC server | Key Management Controller server |
| L&G | Short for Landis and Gyr, the old name of the Siemens Metering company, but a term that is still in general use in Pathway documents. |
| PA | Payment Authorisation |
| PAS | Payment Authorisation Service |
| PMMC | Postmaster's memory card |
| POK | Post Office Key |
| PPP | Point to Point Protocol |
| PRAW | Post office Recovery Application Workstation |
| SHA | Secure Hash Algorithm |
| SI | Software Issue |

| | |
|---|---|
| SIPR | SI Private Key |
| SIPU | SI Public Key |
| TIP | Transaction Information Processing |
| TK | Traffic Key |
| VPN | Virtual Private Network |

## CONTENTS

# 0. INTRODUCTION

## 0.1 Summary

This document examines the management of keys within Pathway, analysing how they are currently managed, and what the requirements are for key management in NR2+.

## 0.2 Background

Cryptography is used in several parts of the ICL Pathway business system to support commercial security. As in all cryptographic systems, integrity depends on adequate management of the keys. Fully integrated, secure and centralised management of the keys is required for future versions of Pathway.

Key management on this scale is not yet common practice. There is no prior art and few theoretical models. Within Pathway there are interim solutions at Release 1c which are largely manual and do not form a consistent integrated system. Nevertheless, these solutions provide valuable lessons for the design of an integrated system.

Given the scarcity of working models, the system requirements must be derived from scratch by extensive analysis. This document is the record of that analysis.

## 0.3 Relationship to [POKM]

This document is being developed in parallel with the post office key management document [POKM].

The scope of this document is wider than the [POKM], which focuses in on management of keys at the post office. That will be a major thread of key management in general, but this document ensures we capture all the threads of key management. This is not incompatible with developing the detail of post office key management.

## 0.4 Terminology

- Over the life of this document, the terms used elsewhere to describe the different releases have evolved. What is now termed NR2 elsewhere, is called NR2 in this document. What is termed NR2+ elsewhere, is called NR2+ in this document.
- The term Key Management System (KMS) is sometimes used in different ways. In some people's understanding it means the general set of processes for Key Management, but to other people it brings images of monolithic automation. In this document we do not use the term KMS at all, instead the following terms are used with the following meanings:

**Key Management** (KM) embraces all the processes and resources, whether automated or human, involved in managing the keys described in this document.

- The term **Key Management Application** (KMA) is used to mean the suite of applications that implement the Key Management Controller, which is the applications and data that constitute the central KM functionality that is distributed among the campuses and the Key Manager's site.
- The term **Key Management Controller server** (KMC server) is used to identify the physical instance of the part of the KMA that is executing at a central campus (with whatever hardware it needs), accessed from the **Key Manager's workstation** (KM workstation).
- In addition, a separate application will be required for off-line certification, this is termed the **Certification Authority Workstation** (CAW).
- The private key component of an asymmetric key pair is managed split into two parts: a **Black Key Set** consisting of the private key (and superfluously its public key) encrypted symmetrically using Red Pike under a symmetric key, used only for that purpose, referred to as the **Red Key**. Each of these

parts is referred to in this document as a **part key**. Neither part is of any value to an attacker without the other.

- The document contains information in tabular form about where each key type is held and how many copies are about. The following terms are used in the tables:

| | |
|---|---|
| Key Type: | Identifies the cryptographic algorithm with which the key is used |
| No of Concurrent Keys: | The number of different key versions that exist at the same time |
| Copies of Each Key in Use: | The number of operational copies of the key that exist (excluding hot standby copies). |
| Record Copies: | Copies kept for recovery purposes by the Key Generator |
| Boot-up Copies: | Copies or part copies on exchangeable material needed for booting up the platforms that use them |
| Frequency of change: | A broad statement of how often the key value is routinely changed. |

The counts given are those planned for NR2+ and are given only as a sizing guideline.

## 0.5 Scope

It is not the intention that this document should be specifying any requirements for cryptography, or cryptographic protection, those have been specified and agreed elsewhere (see list of document cross-references). This document is concerned solely with management of the NR2+ keys already identified to meet those cryptographic requirements. With the exception of the vitally important Certification Authority key, it does not identify any requirements specific to individual key protection keys, whose presence and use are internal design matters. It does however give general requirements relating to the protection of all key material and the impact on business of having to change or revoke any kind of key.

This analysis aims to identify the business and operational requirements for Key Management. It is not the intention here to draw any conclusions about the design or engineering of the system. Neither are any security quality requirements specified, so there is nothing said about any ITSEC or government security evaluation levels that should be aimed for. The emphasis throughout this document is on functionality.

The primary target user of KM is the Pathway Cryptographic Keys Manager (ref. [ACCPOL]) who controls the use of keys and is responsible for generation and distribution of all the keys, rather than the Pathway Key Custodians who administer one or more keys in use at a site.

## 0.6 Approach

Following experience with the Managed Key Service at Release 1c we have drawn a hypothetical model of Key Management and used this as a framework for exploring the requirements. This model is only intended to be an aid. Where it has limitations that conflict with actual requirements, it will not constrain articulation of those requirements.

We have held a series of brainstorming sessions with the Pathway Security product manager, structured around the system model. At these sessions we have gathered a large number of observations about key management problems and requirements. This raw material will be contained in a spreadsheet appended to document [HLD].

This raw material has been sifted to remove repetition and to discover associated themes. We have interpreted the observations and restated them in business-imperative and operational-imperative terms. The resulting statements of requirement are presented in this document for review by Pathway representatives.

Iterative review of this document will produce the agreed requirement set.

## 0.7 Organisation

Section 2 gives some background to the business areas concerned. Section 3 analyses the requirements on key management of specific keys, taking into account the historic state of key management for each key. Section 4 and 5 state the generic requirements of key management from a broader point of view, and from the various perspectives of those affected by key management.

Requirements are categorised into one of three categories, numbered sequentially within category. The categories are:

- Prefix "G": General requirements that apply to more than one key type, in many cases applying to all key types.
- Prefix "H": High level requirements that have an overriding effect on all other requirement types.
- Prefix "P": Requirements on operational procedures.
- Prefix "S": Specific to one key type or to one implementation component that affects no more than one key type.

Each requirement is annotated with its reference number in the form **(Req't: Xnnn)**, where **X** is the type and **nnn** is the number of the requirement within type..

From Formal Issue 2.0 onwards, requirement numbering starts at 1 within each category, with no gaps. If, in future, a requirement is agreed not to apply, it will remain in the document, annotated as being no longer applicable. Its number will not be reused. Other documents, when referring to requirement numbers to show conformance, will continue to list the inapplicable ones annotated as such. If a requirement's meaning changes, the change will be highlighted in the changes lists at the start of this document. The aim is to keep any such changes to a minimum, and to handle a change in this way only if it is slight. It is also possible that, if the change is major, the old requirement will be lifted and replaced by a completely new one with a new number.

Requirements are not necessarily listed in numerical order within type.

The highest numbered general requirement in this version of the document is G108.

The highest numbered high level requirement in this version of the document is H14.

The highest numbered procedural requirement in this version of the document is P9

The highest numbered specific requirement in this version of the document is S92

So this document identifies 223 requirements in total. A small degree of overlap may be noticed, but this has been reduced as far as is practicable.

# 1. BUSINESS SYSTEM

This section gives a deliberately brief overview of the business system in which cryptography is being used, in order to lead into the specific requirements for key management which is the main concern of this document. Cross-reference is made to other documents for detail, rather than repeating it here.

## 1.1 Business Elements Using Cryptography

The Key Business Elements in the system which require the use of cryptography are:

Benefits Payments System

Post Office Counter Infrastructure Services

These provide a series of business application services such as:

- BES (Benefit Encashment Service)
- PAS (Payment Authorisation Service)
- CMS (Card Management Service)
- EPOSS (Electronic Point of Sale Service)
- APS (Automated Payment Service)
- OBCS (Order Book Control Service)

These are described in detail in the [SADD].

In addition there are business requirements demanding cryptography around the administrative aspects of the Pathway systems, in particular the remote software issues and installation system.

## 1.2 Business Benefits

Cryptography is used in these business systems to counter security threats to the Pathway system, ensuring authenticity, confidentiality and integrity of data in the system and limiting the financial risks in running the system.

Different parts of the business, and of the architecture demand different types of cryptography depending on whether the need is for confidentiality or integrity or both. This analysis has already been done (the requirements are in [SFS]) and is not repeated here, as this document is analysing the requirements of key management, rather than the requirements for cryptography.

The analysis/design of the cryptography gives rise to many keys, of different types, in use in the Pathway system. Such sophisticated use of cryptographic techniques demands powerful key management functions in order to realise the business benefits required of key management:

- central key control, maximising the effectiveness of the cryptography in use **(Req't: H1)**
- controlled key changes to minimise opportunity for key compromise **(Req't: H2)**
- managed key handling and distribution to ensure key compromise is minimised **(Req't: H3)**
- rapid response if a key is compromised, minimising the impact of the attack **(Req't: H4)**
- minimising the ongoing costs of managing keys **(Req't: H5)**
- minimising the disruption to the services of cryptography and key management **(Req't: H6)**

The business benefits of smooth management of keys will only be realised if management of all the keys is analysed.

## 1.3 Business Domains

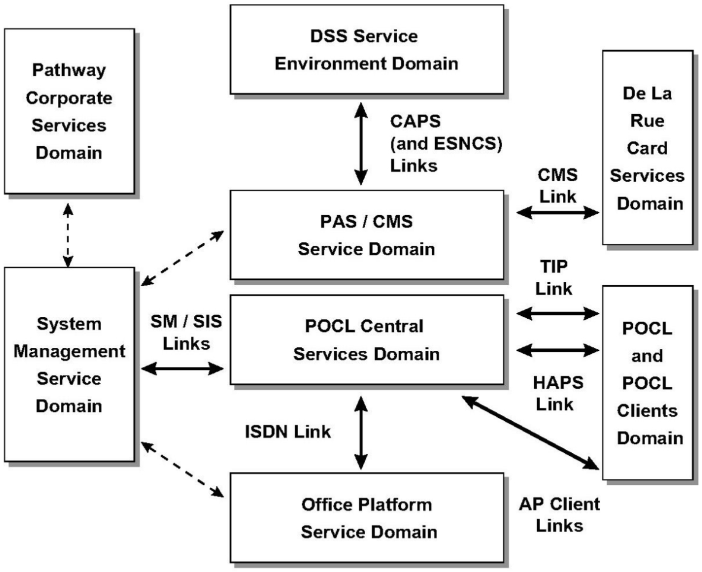
Various parties are involved in the provision of these services including:

- DSS Benefits Agency
- POCL (Post Office Counters Limited)
- POCL Clients:
  - Utilities (Gas, Electric, Water companies)
  - BT (British Telecom)
  - TV Licensing Authority
  - Local Authorities
  - etc.
- DLR (De La Rue)
- ICL Pathway
- CFM (DSD)
- CFM(NI)
- Oracle
- Sequent

## 1.4 Security Domains

The business imperatives of the overall system and the diversity of parties involved have resulted in an architecture with a number of linked domains supporting the operation of the business applications, resulting in security requirements for data in those domains, and on the links between the domains.

The relevant security domains in place to support these applications, and the links between them are shown in the following diagram:


Pathway Corporate Services Domain
DSS Service Environment Domain
CAPS (and ESNCS) Links
De La Rue Card Services Domain
CMS Link
PAS / CMS Service Domain
TIP Link
System Management Service Domain
SM / SIS Links
POCL Central Services Domain
POCL and POCL Clients Domain
HAPS Link
ISDN Link
Office Platform Service Domain
AP Client Links

The domains are described in detail in the [SFS].

## 1.5 Use of Cryptography

The cryptography requirements within the ICL Pathway system fall into 3 areas:

- data on the communication links
- individual messages
- data stored on physically insecure post office filestore

There is a requirement to contain the complexity of the cryptography management by provision of automated key management facilities across these three areas **(Req't: H7)**.

The following sections cover these areas in more detail.

# 2. SPECIFIC KEY MANAGEMENT REQUIREMENTS

## 2.1 CAPS Key

### 2.1.1 Overview

CAPS access service links are used to transfer files, containing mainly payment authorisations, stop notices and customer personal details (including instructions to bring customers onto the service), from BA's (VME) CAPS systems to ICL Pathway's (Sequent) CAPS Access Service (CAS). Information sent back from ICL Pathway to CAPS includes benefit encashments and expired payments, but no encryption is applied in this reverse direction.

The CAPS online service (at NR2) uses the same route and keys, but data is transferred directly, fully encrypted, rather than in files which are partially protected by encryption techniques. This does not affect key handling.

The Electronic Stop Notice Control System (ESNCS) used by the Order Book Control Service (OBCS) will use one of the CAPS links.

The protection on the CAPS link is aimed at reducing the financial risk to ICL Pathway and the Contracting Authorities. The purpose of this protection is integrity and origin authentication.

### 2.1.2 Background

The CAPS systems operate from up to 4 different Area Computing Centres around the country, each of which can have more than one VME mainframe. (Note at R1c this is initially only one VME mainframe, but during the life of R1c this will expand to the above).

ICL Pathway's (Sequent) CAPS Access Service (CAS) runs on a Sequent machine located centrally. (Note there are Wigan and Bootle machines for resilience, but they share one replicated data-store)

Data on the link is protected by encryption of selected (or all) fields, including financial totals under a secret key (the CAPS Key) shared by all the machines on the link, with symmetric encryption by Red Pike algorithm using Cipher-Block Chaining.

Key changes are expected to be approximately every two years, or on key compromise.

### 2.1.3 Key Management at R1c

*2.1.3.1 Generation*

Key material is supplied (on paper) from an off-line key generator, using an alphanumeric format. A checksum is included in the key material to detect typing errors.

*2.1.3.2 Deployment*

Key material is loaded manually and locally into the Series 39 (VME) machines and Sequent platform at each end of the CAPS links. This must be done on the Sequent first, which maintains a 'key ring' with the new and old keys for a defined period of time.

Keys are installed, by the authorised custodians, who type them in. On the Sequent this involves logging in as root.

*2.1.3.3 Storage*

Keys are stored (obfuscated) in a file with file access restricted by use of the operating system access controls. Read and modify access are permitted for the approved custodian with no access permitted for all other users.

The above is true on the Sequent, on VME the key is maintained (obfuscated) in the system catalogue with access (read and write) restricted to one VME username/logon. This username is used to manage the keys and use the keys.

Both systems will have (obfuscated) key copies on system backups.

In addition the key generator maintains a copy of the keys generated. This is kept off-line on a floppy disk in a physical safe. This is needed to encrypt the next key to be generated.

#### *2.1.3.4 Usage*

On the Sequent the cryptographic functions run in 'privileged' mode (i.e. they have access to a special UNIX group which in turn allows them access to the key file). They access the stored keys on each usage of the key.

On VME the cryptographic functions run in the username with access to the key, accessing the stored keys on each usage of the key.

#### *2.1.3.5 Deactivation*

On the VME machines de-activation is immediate on replacement of a key. On the Sequent a 'key ring' is maintained with the new and old keys for a defined period of time, after which the old key is no longer usable. This period is defined at key generation time of the new key.

#### *2.1.3.6 Key Changes*

Key changes are performed at intervals agreed with the Contracting Authorities, based on advice from CESG, for integrity protection.

In practice this involves generating the new key on paper, copying and delivering the papers to appropriate key custodians, and co-ordinating them to ensure the keys are changed in the correct sequence and within the key de-activation period.

### 2.1.4 Key Management Requirement

In NR2:

1. Hardware CAPS key Generation was required to be introduced.
2. No other changes required, key changes continued to be manual.

In NR2+:

1. CAPS keys must be supported in a manner that meets all applicable general requirements **(Req't: S1)**.

### 2.1.5 CAPS Key characteristics summary

| | CAPS Key |
|---|---|
| Key Type | Red Pike Symmetric |
| Key Size | 64 bits(handled as 13 character alphanumeric in places) |
| No of Concurrent Keys | 1 (2 during change-over period) |
| Number of managed copies in use | 6 (one at each of four CAPS sites, and 1 at each Pathway central site). |
| Record Copies | Key Generator keeps 1 copy |
| Managed Key Clients | CAS VME platforms<br>CAS Oracle Sequent platforms |
| Boot-up Copies | None - the value issued on paper is destroyed after use. |
| Frequency of Change | 2 years |

## 2.2 CMS Key

### 2.2.1 Overview

CMS Links are used to transfer card production data and PUN information to the card producer, De La Rue.

There is no explicit Contracting Authority requirement for protection of CMS links. The protection is solely aimed at reducing ICL Pathway's financial risk.

All data on CMS links is encrypted, for confidentiality and integrity, using Red Pike. This enables ISDN lines to be used rather than dedicated links.

At the ICL Pathway end, the CMS file is transferred to a Windows NT platform where the entire file is encrypted using Red Pike. The file is transmitted to the target platform, where it is decrypted again at application level.

### 2.2.2 Background

The data is transferred from the CMS Host Central Server (located at Bootle or Wigan, each backing up the other) to the De La Rue Interface Platform (NT server), located at Wigan/Bootle in clear, using NFS.

Once encrypted the data is sent to the remote machine in bulk.

The remote machines are located at Tewkesbury, and Sittard (in Holland), which acts as a backup. There are two PC's in Tewkesbury, one acting as standby.

Uses the CMS symmetric key (Red Pike).

Key changes are expected to be approximately every two years, or on key compromise.

See [TED] section 5.5

### 2.2.3 Key Management at R1c

#### *2.2.3.1 Generation*

Key material is supplied (on a floppy disk) from an off-line key generator.

#### *2.2.3.2 Deployment*

Key material is loaded manually and locally into the NT machines at each end of the link by inserting the floppy disk into the machine at the right time. This must be done on each boot of the machines

Keys are installed, by the authorised custodians.

#### *2.2.3.3 Storage*

Keys are stored on the floppy disks, and in memory (in clear) at each end of the link.

In addition the key generator maintains a copy of the keys generated. This is kept off-line on a floppy disk in a physical safe. It is recommended that the key manager also stores a spare copy in a safe place.

#### *2.2.3.4 Usage*

The key is used from memory on each encryption/decryption.

#### *2.2.3.5 Deactivation*

Closing down the service (either end) will stop the system using the current key. After editing the registry, that key is no longer active. Destruction of the floppy disks would complete deactivation.

#### *2.2.3.6 Key Changes*

Key changes are performed at intervals agreed with the Contracting Authorities, based on advice from CESG, for integrity protection.

In practice this involves generating the new key on floppy disks, delivering them to the key custodians at each end of the link, and co-ordinating them to ensure the keys are changed in a synchronised manner. This involves closing down the service, editing the registry and re-booting the machines.

### 2.2.4 Key Management Requirement

NR2:

1. Hardware CMS key Generation was required to be introduced.
2. No other changes required, key changes continued to be manual.

NR2+:

1. CMS keys must be supported in a manner that meets all applicable general requirements **(Req't: S2)**.

There is no specific requirement to change CMS key management to bring it in line with FTMS-based key management, but it is likely that this will happen.

### 2.2.5 CMS Key characteristics summary

| | CMS Key |
|---|---|
| Key Type | Red Pike Symmetric (also used to authenticate) |
| Key Size | 64 bits |
| No of Concurrent Keys | 1 |
| Number of managed copies | 4. One at each end of the CMS link from each Pathway campus |
| Record Copies | Key Generator keeps 1 copy |
| Managed Key Clients | CMS DLR local gateways<br>CMS DLR remote gateways |
| Boot-up Copies | 4 - one at each end of each link |
| Frequency of Change | 2 years |

## 2.3 CHAP Key

### 2.3.1 Overview

Up to and including NR2, CHAP keys are used to protect the ISDN links between the POCL central services domains to the Post Offices.

CHAP is a PPP challenge and authentication protocol that ensures at call set-up, and subsequent handshakes, that there is a genuine caller at the other end.

### 2.3.2 Background

CHAP initial connection authentication is provided, with refresh,  supplemented by CLI authentication of the Post Offices from the ICL Pathway campus. CHAP re-authentication is applied to all calls (however initiated).

The CHAP protocol is implemented centrally by Cisco routers, and at the Post Offices by ISDN Adapters (EICON Cards) in each Gateway machine.

Other protection is/will be applied to individual messages sent across these link, namely:

- Payment Authorisations (PA keys)
- Software issue (SI keys)
- Automated Payments (AP keys)

### 2.3.3 Key Management at R1c

#### *2.3.3.1 Generation*

Key material has been generated by The Solution Centre, as 40,000 CHAP values, supplied with an index and supplied securely, on floppy disk, to the Boot-servers (via Tivoli) and CFM for configuration in the Routers.

#### *2.3.3.2 Deployment*

The routers are configured with the values by CFM, under instructions supplied from the Auto-config database.

The Post Office machines receive their CHAP key (obfuscated) from the Boot server when the gateway machine at the Post Office is brought on-line.

*2.3.3.3 Storage*

Pre-deployment, the CHAP keys are stored by CFM, and in the Boot server machines.

During use they are stored on the Cisco router, and on the Gateway PC. On the Gateway PC persistent storage of the Chap key is achieved by recording it in the NT Registry.

If the current value of the Chap Key is Chap1 then the value recorded in the NT registry is Edes56k(Chap1), where Edes56k is the result of applying the Des algorithm in CBC mode using a 56 bit key k. The key k is hard coded in the NDIS driver (.sys file).

*2.3.3.4 Usage*

Used directly by the Cisco router and the EICON card whenever authentication is performed.

*2.3.3.5 Deactivation*

None.

*2.3.3.6 Key Changes*

No key changes are possible

### 2.3.4 Key Management Requirement

NR2:

1. It was required that it should be possible to change the CHAP key on suspected key compromise.

NR2+:

No requirement for CHAP, which is replaced by VPN.

## 2.4 VPN Key

CHAP is superseded in NR2+ by VPN technology. Under the VPN regime, all links between post offices and the central campuses will be encrypted and channelled through central VPN Gateway Security Servers (referred to below as VPN Servers). Participating post offices and VPN Servers will be authenticated as valid members of the Pathway community. Post offices must not be able to masquerade as VPN Servers **(Req't: S2)**. Post offices and VPN Servers authenticate using RSA private keys with public key certificates (the combination is referred to as the VPN Key). Private keys destined for central VPN servers are distributed over an automatic link under the protection of a PIN created by the VPN product, the PIN being distributed manually. Post office private VPN keys are not dependent on PIN protection, they are distributed under the protection of the key management scheme. The certificates will be signed by a special purpose Certification Authority, different from the CA used for other Pathway public keys. The symmetric VPN encryption key is generated dynamically by the bought-in VPN technology as required, and is not separately managed by the Pathway key management regime. During the boot phase of a new post office, a special global non-secret key value (the VPN Exception Key) is transiently used to enable a post office to communicate via the VPN Servers to the KMC server and obtain its regular VPN Key. Communication using the Exception Key must be limited at the centre to the KMC server only, and then only if pre-authorised **(Req't: S4)**.

Pre-NR2+

Deployment of VPN may be done before NR2+ during NR2 for non-security reasons. If this happened, a requirement relating to such an early deployment would be:

1. A single global VPN key is acceptable, with no confidentiality requirement associated with it, but it must be configured so that it can continue to be used in NR2+ for the exception route into the KMC server, avoiding the need for a global replacement of one key with another **(Req't: S6)**.

NR2+:

1. The CHAP authentication requirement is superseded by VPN technology, which is supported on all post office links **(Req't: S7)**.
2. Routine VPN Key changes will be managed and performed automatically under the control of the KMA **(Req't: S8)**
3. Each post office member of the VPN community must have a different operational key value **(Req't: S9)**.
4. Automatic VPN key changes occur at times in line with other Pathway key expiry periods **(Req't: S5)**.
5. The Exception Key is required to be managed like any other configuration data **(Req't: S10)**. There are no special confidentiality requirements relating to it and it is not considered further in this document.
6. The VPN security regime must be able to recover from any communications breakdown that the regime may erroneously cause, in particular through errors in key management, within time-scales conformant to network serviceability commitments **(Req't: S16)**.

### 2.4.1 VPN Key characteristics summary

| | **VPN Key** |
|---|---|
| Key Type | RSA private/public key pair, the public key being contained in a certificate signed by the VPN CA. |
| Key Size | 1024 bits |
| No of Concurrent Keys | 20,000 + one shared between the central VPN servers |
| Number of managed copies | 1, at each participating VPN node. |
| Record Copies | Key Generator keeps 1 copy, autoconfig keeps 1 |
| Managed Key Clients | PO gateway workstations<br>VPN Servers |
| Boot-up Copies | 1 in the Key File of the VPN software on each gateway PC and VPN Gateway Server |
| Frequency of Change | 2 years |

## 2.5 Post Office Filestore Encryption Key (FEK)

### 2.5.1 Overview

Nominated files on Post Office workstations and gateway machines are automatically encrypted at disk access level to preserve data confidentiality in the event of the workstation being stolen

### 2.5.2 Background

None of the NT workstations installed in Post Offices will have operable floppy disk drives (since, if fitted, they will be physically blanked off and disabled in the BIOS). The workstations will be rolled out to the sites with the majority of the software, including the cryptography software, pre-configured in the factory.

Protection of filestore will be applied after delivery on site **(Req't: S11)**.

The Post Office Manager (or authorised representative) will normally be the only person on site who has the means of unlocking the key to the filestore encryption, and it must be technically possible to control this **(Req't: S12)**. He/she is not, however, required to be IT literate since the procedures used will be straightforward and well documented **(Req't: S13)**.

In general each workstation will be used by a different counter clerk who will use other authentication data to sign on to the workstation. Counter clerks must not be able to unlock the filestore without assistance from the Post Office Manager **(Req't: S14)**. Workstations are expected to be left running continuously, twenty four hours a day seven days a week; power down causes filestore to be locked, and this must be unlocked on power up, though the need to do this can be assumed to be an exceptional occurrence **(Req't: S15)**. However, counter clerks will sign on and off at more frequent intervals.

### 2.5.3 Key Management at R1c

#### *2.5.3.1 Generation*

Key material is generated by software entropy on the Post Office gateway machine at rollout time.

#### *2.5.3.2 Deployment*

Deployment is done in two forms:

1. Having generated the key value, it is transferred to the postmaster's memory card (PMMC) during rollout, where it is protected by a PIN.
2. To deploy ready for use, the postmaster inserts the PMMC in each PC in the Post Office as it is booted up.

#### *2.5.3.3 Storage*

The FEK is stored on the PMMC.

In the event of a PMMC or PIN being lost, the FEK can be recovered by use of the 'verbal Diffie-Hellman' exchange. This involves the postmaster contacting the help desk, authenticating himself to them, reading a series of 16 rows of 15 alphanumeric characters (the Recovery Code) to the help desk, which uses the PRAW to generate a 15 character Recovery Key. This is then recited back to the postmaster, who enters it into the PC. The FEK is then re-created and written to a new card.

#### *2.5.3.4 Usage*

Used from memory by the Team-Crypto software as encryption/decryption is performed.

#### *2.5.3.5 Deactivation*

None.

#### 2.5.3.6 Key Changes

No key changes are possible except by performing a recovery (See Section 2.5.3.3).

### 2.5.4 Key Management at NR2

#### 2.5.4.1 Generation

As R1c, but a Recovery value is transmitted to the help desk via Tivoli to ease recovery from a lost PMMC.

#### 2.5.4.2 Deployment

As Release 1c.

#### 2.5.4.3 Storage

As Release 1c

#### 2.5.4.4 Usage

As Release 1c

#### 2.5.4.5 Deactivation

None.

#### 2.5.4.6 Key Changes

No key changes are possible except by performing a recovery (See Section 2.5.3.3).

### 2.5.5 Key Management at NR2+

#### 2.5.5.1 Generation

Key material is generated centrally and issued to post offices over the Interactive Channel.

#### 2.5.5.2 Deployment

As earlier releases, except the key is delivered over the Interactive Channel to the gateway PC.

#### 2.5.5.3 Storage

As earlier releases.

#### 2.5.5.4 Usage

As Release 1c

#### 2.5.5.5 Deactivation

None.

#### 2.5.5.6 Key Changes

At prescribed intervals over the Interactive Channel.

### 2.5.6 Key Management Requirement

NR2:

1. The verbal Diffie-Hellman recovery mechanism was improved, to greatly reduce the volume of numbers, which had to be exchanged.
2. There was a requirement to be able to change the FEK at NR2 on suspected compromise.

NR2+:

1. FEK keys must be supported in a manner that meets all applicable general requirements **(Req't: S18)**.

### 2.5.7 FEK Key characteristics summary

| | FEK |
|---|---|
| Key Type | Red Pike Symmetric |
| Key Size | 64 bits |
| No of Concurrent Keys | 20,000 |
| Number of managed copies | 1 per post office platform |
| Record Copies | KMC server keeps 1. (pre-KMA, the PRAW keeps root) |
| Managed Key Clients | |
| Boot-up Copies | 1 on the PMMC |
| Frequency of Change | 2 years |

## 2.6 PA Key

### 2.6.1 Overview

The PA Key is used to preserve the integrity of Payment Authorisations as they are transferred from the Pathway central sites to the post offices, which process them.

### 2.6.2 Background

The PA key is public- private asymmetric key pair. The private key exists as a black key set, protected by a red key.

PA signature keys reside on PA Agent servers. As the red key is kept off-line, it is introduced on each boot of the servers. This involves co-operation of CFM key custodians (local) and server administrators (remote).

This requires the Pathway key custodian to distribute red key floppy disks to a CFM key custodian for each server/server location.

### 2.6.3 Key Management at R1c

#### *2.6.3.1 Generation*

The public/private key pair is generated by TSC. No certification is involved. Ten sets have been pre-generated for R1c.

#### *2.6.3.2 Deployment*

The (first) private black key set is distributed by D2D (issued via CM) to the Vector server(s) and the PA signing agent(s).

The (first) red key is copied (on floppy disk) by the Pathway key custodian to each CFM key custodian, who introduces it on each boot of the server.

The public keys (all 10 of them) are distributed via CM and D2D to the post office (pre-configured)

#### *2.6.3.3 Storage*

Black key set 1 - in filestore on the servers using it. Others in secure storage held by TSC.

Red Key 1 - on floppy disks in secure safes at each location. Others in secure storage held by TSC.

Public keys - on filestore in the post office machines. (All 10)

#### *2.6.3.4 Usage*

Used from memory by the signing agents as required for signing payment files, and by the post offices from key file or key store as required to verify the payment files.

#### *2.6.3.5 Deactivation*

Only by explicit removal by manual intervention using Tivoli.

Red key floppy disks are destroyed.

#### *2.6.3.6 Key Changes*

A primitive form of key changing is possible at R1c. It requires human intervention and co-operation between TSC, the Pathway key manager, local CFM key custodians and server administrators.

TSC staff get a new black key set and red key from secure storage, and get the black key set issued via CM to the PA signing server. Note it is not defined how this process is timed or how to check it has completed. An administrator is required to check the black key set has arrived on the server.

The red key is then distributed by the Pathway Key Manager to the local key custodian, who can then co-operate with the server administrator to close down the service, edit the registry to introduce the new key, and re-boot the server to start using the key.

The post offices will then be able to check the signatures using any of the keys used so far, unless the copy of the key at the post office is explicitly destroyed by manual use of Tivoli (i.e. there is no automatic time-out of keys).

### 2.6.4 Key Management Requirement

NR2:

1. Hardware key generation was required to be introduced.

NR2+:

2. PA keys must be supported in a manner that meets all applicable general requirements **(Req’t: S20)**.

### 2.6.5 PA Key characteristics summary

| | PA Key |
|---|---|
| Key Type | Public-Private Asymmetric DSA Key Pair |
| Key Size | 768 bits |
| No of Concurrent Keys | 1 active private key (2 during changeover period) with corresponding public key certificate(s). . There may be a number of additional certificates held at a post office in anticipation of yet to be used private keys. This number may vary. Any corresponding private keys will be kept in high security off line storage. |
| Number of managed copies | L copies of private key part pairs,<br>where L = the number of BPS payment loader platforms.<br>≤40,000 copies of the certificate for each public key, one per post office counter workstation in service. |
| Record Copies | Key Generator keeps one copy |
| Managed key clients | PO Counter workstations<br>BPS payment loader platforms |
| Boot-up Copies | 2, one at each Pathway campus |
| Frequency of Change | 2 years |

## 2.7 SI Key

### 2.7.1 Overview

The SI Key is used to preserve the integrity of Software issues as they are transferred from the Pathway central sites to the post offices, and to other servers being configured. It is also used on personalised autoconfig files sent to post offices at rollout.

### 2.7.2 Background

The SI key is public-private asymmetric key pair. The private key exists as a black key set, protected by a red key.

SI signature keys reside on the SI signature server, located in Feltham and on an autoconfig signing server at each of the central Pathway campuses. As the red key is kept off-line, it is introduced on each boot of the servers. This involves co-operation of CFM key custodians (local) and server administrators (remote).

In Release 1c, SI public keys reside on a number of verifying servers. The current list of these servers is (or is expected to be during the life of R1c):

- All participating post offices
- CFM Software Depot (Wigan and Bootle)
- Pathway CS Software depots (Bracknell)
- SSC Live rig (Bracknell)
- Live Support rig (Bracknell)

- GiroBank NT 'receiver' box (for PMS/CMS help desks)

There are likely to be others later.

### 2.7.3 Key Management at R1c

#### *2.7.3.1 Generation*

The public/private key pair is generated by TSC. No certification is involved.

#### *2.7.3.2 Deployment*

The private black key set is hand installed to the SI and autoconfig signing agents from a floppy disk.

The red key is copied (on floppy disk) by the Pathway key custodian to a CFM key custodian, who introduces it on each boot of the server.

The public key is distributed via CM and D2D to the post office, and other servers using it.

#### *2.7.3.3 Storage*

Black key set - in filestore on the server using it.

Red Key - on floppy disk in secure local safe.

Public key - on filestore in the post office machines, and other servers using it.

#### *2.7.3.4 Usage*

Used (from installed black set and red-key floppy disk) by the signing agent when signing software issue packages, and by the post offices (and other servers) from filestore/key store as required to verify the payment files.

#### *2.7.3.5 Deactivation*

None - other than moving forward to new keys, and therefore abandoning old key files, unless the copy of the key at the post office is explicitly destroyed by manual intervention using Tivoli.

Red key floppy disks are destroyed.

#### *2.7.3.6 Key Changes*

A primitive form of key changing is possible at R1c. It requires human intervention and co-operation between TSC, the Pathway key manager, local CFM key custodians and server administrators.

TSC staff get a new black key set and red key from secure storage, and get the public key issued via CM to the other verifying servers (not the post offices which already have the public keys). Defining the servers is a manual process. Note it is not defined how this process is timed or how to check it has completed - presumably someone (e.g. administrator) would have to check the black key set has arrived on each server.

The red key and black key set is then distributed by the Pathway key manager to the local key custodian, who can then co-operate with the server administrator to install the black key set on the SI signing server and edit the registry to introduce the new key to start using the new key. Re-booting is not necessary.

The post offices will then be able to check the signatures using any of the keys used so far, unless a key is explicitly destroyed by manual use of Tivoli (i.e. there is no automatic time-out of keys). Note that signed messages can exist for long periods (months) in depots and therefore messages can come through with 'old' signatures on.

### 2.7.4 Key Management Requirement

NR2:

1. Hardware SI key generation was required to be introduced.

NR2+:

3. SI keys must be supported in a manner that meets all applicable general requirements **(Req't: S22)**.

### 2.7.5 SI Key characteristics summary

| | SI Key |
|---|---|
| Key Type | Public-Private Asymmetric DSA Key Pair |
| Key Size | 768 bits |
| No of Concurrent Keys | 1 private key part pair (2 during changeover period) with corresponding public key certificate(s).<br>There may be a number of additional certificates held at a post office in anticipation of yet to be used private keys. This number may vary. Any corresponding private keys will be kept in high security off line storage. |
| Number of managed copies | Private Key part pairs: 3<br>≤40,000 copies of the certificate for each public key, one per post office counter workstation in service. One for each Tivoli-managed platform other than post office ones. |
| Record Copies | Key Generator keeps one copy |
| Managed key clients | PO counter workstations<br>CM signing server platforms<br>Tivoli-serviced platforms on the Pathway LANs |
| Boot-up Copies | 3 (private keys) |
| Frequency of Change | 2 years |

## 2.8 Rambutan Keys

### 2.8.1 Overview

Various links are protected by hardware encryption/decryption devices. The devices in ICL Pathway's solution are types ED600RTS and ED2048R3 supplied by Zergo.

These devices are certified products (ITSEC) and provide cryptographic protection using CESG designed Rambutan crypto-kernel.

The links protected by these devices are:

- ICL DSD (help desk) links from STE04, LSA01 and FCY03 to Wigan and Bootle.
- ICL CFM (systems mgt) links from Belfast and Ste04 to Bootle and Wigan.
- ICL Pathway HQ links from FEL01 to Wigan and Bootle
- POCL HAPS Link

### 2.8.2 Key Management at R1c

The Zergo encryptors have in-built key management. The Zergo encryptors operating instructions contain a section on key management and that has been incorporated as part of CFM's operating instructions.

CFM provide management of the Zergo units (and their keys) as a service. The keys are sourced directly from CESG.

### 2.8.3 Key Management Requirement

Management of Rambutan keys should follow accepted practice already established in other contexts for the products that use them **(Req't: P1)**. In NR2+ automated prompts to the Cryptographic Key Manager to remind about the need for a key change are required **(Req't: S24)**.

### 2.8.4 Rambutan Key characteristics summary

| | **Rambutan Keys** |
|---|---|
| Key Type | Rambutan |
| No of Concurrent Keys | 2 per link |
| Copies of Each Key in Use | 2 (1 at each end) |
| Record Copies | 0 |
| Managed key clients | The bought in product platforms come with their own key management regime. The links that they protect are listed in Section 2.8.1. |
| Backup Copies | 0 |
| Frequency of Change | 2 years |

## 2.9 AP Keys

### 2.9.1 Overview

AP keys are used for protection of automated payment records. The AP private key is used at the post office to sign the automated payment message, and the signature verified prior to it being stored on the AP host with the signature removed.

### 2.9.2 Background

The AP key is public-private asymmetric key pair. The private key will exist as a black key set, protected by a red key. The public key is contained in a certificate signed by the CA.

A message will be signed by the post office, using the private key (APPR), which should be unique to the post office.

The AP message, having been signed by the post office is delivered to the Pathway central site as a Riposte message, issued across the post office network, where it is received by the APS agent, which verifies the signature, removes it, and then forwards the unsigned message on to the APS Host machine.

The APS Host will then forward it on to the appropriate utility using FTMS (See Section 2.15).

### 2.9.3 Key Management at R1c

None - AP keys are not used in R1c

### 2.9.4 Key Management at NR2

None - AP signing is not in NR2.

### 2.9.5 Key Management at NR2+

*2.9.5.1 Generation*

Public/private key pairs are generated by the KMC. The CAW creates a public key certificate for each public key.

*2.9.5.2 Deployment*

The private component is distributed over the automatic channel to post offices, each post office having its own unique key.

The public key certificate is distributed over the automatic channel to central campus verifiers.

*2.9.5.3 Storage*

The private key is held encrypted in the Riposte journal.

The public key is held in self-protecting certificates.

*2.9.5.4 Usage*

The private component is used at post offices to sign automated payment transactions. The public component is used at for verifying these signatures at central campus verifying platforms

*2.9.5.5 Deactivation*

By certificate expiry and issue of new private keys and certificates as required.

*2.9.5.6 Key Changes*

Via the automatic channel at prescribed intervals.

### 2.9.6 Key Management Requirement

Releases 1c and NR2:

None – not implemented.

NR2+:

AP keys must be supported in a manner that meets all applicable general requirements **(Req't: S25)**.

### 2.9.7 AP Key characteristics summary

| | **AP Keys** |
|---|---|
| Key Type | Public-Private Asymmetric DSA Key Pair |
| Key Size | 768 bits |
| No of Concurrent Keys | Up to 20,000 key pairs (one per post office) |
| Number of managed copies | 1 private key part pair per counter workstation in the owning post office.<br>H copies of the public key certificate for an AP key, where H = number of AP harvester agent platforms |
| Managed key clients | PO counter workstations<br>AP harvester agent platforms |
| Record Copies | 1 |

| | |
|---|---|
| Boot-up Copies | None |
| Frequency of Change | 2 years |

## 2.10 CA Key

### 2.10.1 Overview

The Certification Authority (CA) key is used to certify the public keys of various other asymmetric keys by signature of a public key certificate. It certifies that the public key in the certificate is a genuine Pathway key and not a spoof.

The CA key is the most trusted key in the system.

### 2.10.2 Background

The CA key is a public-private asymmetric key pair. The private key will exist as a black key set, protected by a red key. The public key is not contained in a certificate as no higher authority exists to certify it.

The CA key is to be a longer key than other keys and therefore to have a significantly longer period of validity than other keys in the system (e.g. 8 years instead of 2).

The CA private key (CAPR) is the most trusted and most protected key in the Pathway system, and therefore is never allowed to go online to a networked machine. It is used solely in the off-line CA workstation (CAW), and is kept locked up in the most secure safe available.

CAPUs will be pre-generated and issued in a batch (designed to last a very long time) to post offices and other verification platforms as part of their pre-installed package, with the regular re-issue, for validation purposes only, for checking they are still correct.

### 2.10.3 Key Management at R1c

A 768-bit CA key has been generated and the CAPU issued to all post offices, but the key is not used at all. The CAPR is held in secure storage.

### 2.10.4 Key Management Requirement

NR2:

Not used.

NR2+:

1. CA keys must be supported in a manner that meets all applicable general requirements **(Req't: S26)**.

There are also additional requirements in NR2+, specific to CA key material:

2. CA keys must be at least 1024 bits long **(Req't: S27)**.
3. The lifecycle for a CA key is longer than that of other keys (of the order of 8 years). The CA signing key must be able to be changed with that frequency, and on suspicion of compromise **(Req't: S28)**.
4. It must be possible to alert post offices, in a time-scale of the order of that taken by the broadcast of an urgent Riposte message, that no further certificates signed by a given CA key should be accepted **(Req't: S29)**.
5. This alerting must not be able to be spoofed **(Req't: S30)**.

6. The confidentiality of CAPR must be protected such that it cannot be attacked on-line, and that no single physical compromise of media or equipment could compromise the key's confidentiality **(Req't: S31)**.
7. Key changes timed by KMA or manually instigated must be possible, but only within the pre-issued key stock **(Req't: S32)**.
8. Regular retransmission of check values for CAPU keys must be supported, for recipients to ensure that local copies have not been tampered with **(Req't: S33)**. The frequency should be configurable, but intervals of the order of 2 or 3 months are appropriate. Some degree of randomnity should be able to be introduced either manually or automatically **(Req't: S34)**.
9. CAPUs are required to be supported on all platforms that verify certificates **(Req't: S35)**.
10. Post office platforms not possessing the full set of CAPU values can be sent them using Tivoli, but the values must be integrity checked at installation time **(Req't: S37)**.

### 2.10.5 CA Key characteristics summary

| | CA Key |
|---|---|
| Key Type | Public-Private Asymmetric Key Pair |
| Key Length | 1024 bits |
| No of Concurrent Keys | 1 private key.<br>up to 10 public keys at each signature verification platform (see below for list). |
| Number of managed copies | Private key part pairs - 1, on the CA workstation<br>Public Key - one copy for every platform that verifies signatures (post office PCs, the CAW, AP Harvester Agents, Tivoli client platforms, FTMS verification platforms, counter application client platforms, the KMC server itself). |
| Record Copies | None |
| Frequency of Change | 8 years |

## 2.11 KI Key

### 2.11.1 Overview

The Key Issue (KI) key is a key used to protect the integrity of the exchanges between the central key management application and other servers communicating with it (mainly post offices). It convinces the communicating servers that they are dealing with a genuine Pathway key management agent.

It is not a business-related key, but a part of the anticipated solution and is documented here only for completeness.

### 2.11.2 Background

The KI key is public-private asymmetric key pair. The private key exists as a black key set, protected by a red key. The public key will be protected by certification by the CA key.

### 2.11.3 Key Management at R1c

None - the KI key is not used at R1c.

### 2.11.4 Key Management at NR2

None - the KI key is not used at NR2.

### 2.11.5 Key Management Requirement

1. As necessary to support other requirements.

### 2.11.6 KI Key characteristics summary

| | KI Keys |
|---|---|
| Key Type | Public-Private Asymmetric DSA Key Pair |
| Key Length | 768 bits |
| No of Concurrent Keys | 1 private key part pair and corresponding public key certificate (transmitted with the signed data it is needed for). |
| Copies of Each Key in Use | Private Key - 2, one at each Pathway site. Public Key – 2, one at each Pathway site |
| Record Copies | Key Generator keeps one copy |
| Boot-up copies | none |
| Frequency of Change | 2 years |

## 2.12 Post Office Key (POK)

### 2.12.1 Overview

The post office key is used to authenticate the identity of a post office when it communicates with the KMA. It is not used until NR2+.

### 2.12.2 Background

The POK will be a symmetric Red Pike key, with an associated key identifier (POKID), used to tell the KMA which key has been used to authenticate.

It is expected that it will be delivered initially to the post office machines via the boot server, but since this route can at best obfuscate its value during transmission, it must be immediately replaced by a securely transmitted value from the KMA during a subsequent phase of rollout.

Changing of POKs is required to be controlled automatically by the KMA.

### 2.12.3 Key Management at R1c

- None - this key does not exist at R1c

### 2.12.4 Key Management at NR2

- None - this key does not exist at NR2

### 2.12.5 Key Management Requirement

NR2

- None - this key does not exist at NR2

NR2+:

1. POKs must be supported in a manner that meets all applicable general requirements, except a transient initial relatively insecure POK may be transmitted to the post office obfuscated, instead of encrypted **(Req't: S38)**.
2. The first secure (properly encrypted in transmission) value of POK must be established during rollout **(Req't: S39)**.

### 2.12.6 POK Key characteristics summary

| | **POKs** |
|---|---|
| Key Type | Symmetric Red Pike |
| Key Size | 64 bits |
| No of Concurrent Keys | 20,000 |
| Number of managed copies | 2 - one at the KMC server and one at the PO gateway PC |
| Record Copies | none |
| Managed key clients | PO Gateway workstations |
| Boot-up Copies | 1, on the PMMC |
| Frequency of Change | 2 years |

## 2.13 Communications Key (CK)

### 2.13.1 Overview

The communications key (CK) will be used to protect confidential key data going up the line from the KMC server to the post office over the interactive key distribution channel. It is not a business-related key, but one anticipated as part of the final solution and is identified here only for completeness.

It will be created simultaneously at both ends of the link via a Diffie-Hellman exchange.

There will be CK generated and used for each interactive exchange for each post office in operation.

### 2.13.2 Background

The CK will be a symmetric red pike key directly derived from a Diffie-Hellman shared secret.

### 2.13.3 Key Management at R1c

None - the key is not used at R1c.

### 2.13.4 Key Management at NR2

None - the key is not used at NR2.

### 2.13.5 Key Management Requirement

1. As necessary to support other requirements.

### 2.13.6 CK Key characteristics summary

| | CK |
|---|---|
| Key Type | Symmetric Red Pike key dynamically generated using a Diffie-Hellman exchange |
| Key Length | 64 bits |
| No of Concurrent Keys | 20,000 |
| Copies of Each Key in Use | 2 |
| Record Copies | none |
| Managed Key Clients | This is not a managed key in the sense that the other keys are managed; it is a transient value, automatically generated and controlled and used for one interactive exchange only. |
| Boot-up Copies | none |
| Frequency of Change | a new key is generated for every post office key management exchange. |

## 2.14 Traffic Key (TK)

### 2.14.1 Overview

The traffic key (TK) will be used to protect confidential key material. It protects material transmitted over the automatic Riposte channel from the KMC server to all destinations served by automatic channels. It is not a business-related key, but one anticipated as part of the final solution and is identified here only for completeness.

For post office destinations, it is transmitted over the interactive channel, protected using CK, from where it is transferred to the PMMC. The PMMC is the medium by which it is transferred to the non-gateway PCs where it is used to decrypt key material arriving via the Riposte based automatic channel. It is transmitted to non-post office destinations by manual means on an exchangeable medium.

There will be TKs for each automatic channel in operation.

### 2.14.2 Background

The TK will be a symmetric red pike key.

### 2.14.3 Key Management at R1c

None - the key is not used at R1c.

### 2.14.4 Key Management at NR2

None - the key is not used at NR2.

### 2.14.5 Key Management Requirement

1. As necessary to support other requirements.

### 2.14.6 TK Key characteristics summary

| | TK |
|---|---|
| Key Type | Symmetric Red Pike key generated at the KMC server |
| Key Length | 64 bits |
| No of Concurrent Keys | up to 20,000 |
| Copies of Each Key in Use | 2 |
| Record Copies | none |
| Managed Key Clients | Post office gateway and non-gateway PCs |
| Boot-up Copies | 1, on the PMMC or non-post office equivalent, which may contain both current and previous values |
| Frequency of Change | of the order of two years. |

## 2.15 FTMS Key for POCL AP clients

### 2.15.1 Overview

This key type will not be used until NR2+. It will be used to protect the integrity and data origin of data transferred directly from Pathway central sites to the POCL AP clients (rather than via the POCL HAPS link as at NR2).

### 2.15.2 Background

The protection takes the form of signing of whole files, the public keys being held in certificates and shipped with each file. It is the objective to make it as similar as possible to the POCL Tip link, though it is only provided in the outward direction.

### 2.15.3 Key Management at R1c

None - not used until NR2+.

### 2.15.4 Key Management at NR2

None - not used until NR2+.

### 2.15.5 Key Management at NR2+

*2.15.5.1 Generation*

Public/private key pairs are generated by the KMC. The CAW creates a public key certificate for each public key.

*2.15.5.2 Deployment*

Both the private component and its corresponding public key certificate are distributed over the automatic channel to FTMS agent platforms on the central campus.

*2.15.5.3 Storage*

The private key is held encrypted in the Riposte journal.

The public key is held in self-protecting certificates.

*2.15.5.4 Usage*

The private component is used at FTMS agent platforms on the central campus to sign files of data for transmission to remote AP client sites. The corresponding public key certificate is then transmitted with each file to be verified. The public component is then used at for verifying the file signatures at central campus verifying platforms.

*2.15.5.5 Deactivation*

By certificate expiry and issue of new private keys and certificates as required.

*2.15.5.6 Key Changes*

Via the automatic channel at prescribed intervals.

### 2.15.6 Key Management Requirement

Releases 1c and NR2

1. None – not used.

NR2+:

4. FTMS keys must be supported in a manner that meets all applicable general requirements **(Req't: S40)**.

### 2.15.7 FTMS Key characteristics summary

| | FTMS Key |
|---|---|
| Key Type | Public-Private Asymmetric DSA Key Pair |
| Key length | 768 bits |
| No of Concurrent Keys | 1 |
| Number of managed copies | 2 private key parts, one on each site client gateway<br>2 Public Key certificates, one on each site client gateway |
| Record Copies | Key Generator keeps one copy |
| Managed key clients | Pathway gateways |
| Boot-up Copies | 2 - one for each site at the Pathway end |
| Frequency of Change | 2 years |

## 2.16 POCL TIP Link

### 2.16.1 Overview

The POCL TIP links are used to transfer information to and from POCL. They carry the entirety of POCL's outlet transaction business and stock data, plus reference data back to ICL Pathway. There is an explicit Contracting Authority requirement for integrity protection of this link in both directions.

### 2.16.2 Background

The POCL TIP link is used to transfer files of data using an FTMS service between the central Pathway sites, and Pathway-supplied NT boxes on the POCL site(s).

The protection takes the form of signing of whole files, the public keys being held in certificates and shipped with each file.

The POCL TIP receiving machines (at each end) will be able to check the integrity of the received files using the public keys held in certificates verified by pre-installed CA public keys. A mechanism will be required to enable the CAPUs to be checked periodically (similar to post office CAPU checks).

### 2.16.3 Key Management at R1c

None - this key is not used at R1c.

### 2.16.4 Key Management at NR2

As for SI keys, though the destination platforms are the platforms that terminate the POCL TIP link.

### 2.16.5 Key Management at NR2+

*2.16.5.1 Generation*

Public/private key pairs are generated by the KMC. The CAW creates a public key certificate for each public key. Each end of the POCL TIP link has a private public key pair generated for it.

*2.16.5.2 Deployment*

Both the private components and their corresponding public key certificates are distributed over the automatic channel to their respective ends of the POCL TIP link.

*2.16.5.3 Storage*

The private keys are held encrypted in the Riposte journal.

The public keys are held in self-protecting certificates.

*2.16.5.4 Usage*

The private component at each end is used by that end to sign files of data for transmission to the other end. The corresponding public key certificate is then transmitted with each file to be verified. The public component is then used at for verifying the file signatures at the receiving end.

*2.16.5.5 Deactivation*

By certificate expiry and issue of new private keys and certificates as required.

*2.16.5.6 Key Changes*

Via the automatic channel at prescribed intervals.

### 2.16.6 Key Management Requirement

Release 1c

None

NR2

1. Manual key changes were supported, using couriered hard media.
2. Remote keys were changed by introducing new key media (private key).
3. Central keys were changed the same way.

There was no certification in NR2.

NR2+:

5. POCL TIP keys must be supported in a manner that meets all applicable general requirements **(Req't: S44)**.

### 2.16.7 POCL Tip Link Key characteristics summary

| | POCL Tip Key |
|---|---|
| Key Type | Public-Private Asymmetric DSA Key Pair |
| Key length | 768 bits |
| No of Concurrent Keys | 2 (one for each direction) |
| Number of managed copies | Private key part pair - 1 (2 if at the Pathway end - one on each site)<br>Public Key certificate - 1 (2 if at the Pathway end - one on each site) |
| Record Copies | Key Generator keeps one copy |
| Managed key clients | POCL platform (TIP and Reference Data)<br>Pathway gateways for the above |
| Boot-up Copies | 3. One at the client end, one for each site at the Pathway end |
| Frequency of Change | 2 years |

## 2.17 Additional FTMS Domains

### 2.17.1 Background

FTMS links are already used in a number of business and system contexts and the use of FTMS will be extended into new areas over time. The management of the cryptographic keys to support the securing of these new links will similarly need to be extended.

### 2.17.2 Key Management Requirement

NR2

It was required to be made possible to support the provision of key material for the FTMS link between the Pathway campuses for the purpose of encrypting Archive Server traffic. This was a first example of the more general requirement that applies in NR2+.

NR2+

It must be possible to support additional secure logical FTMS links between the same or other physical endpoints in new protection domains, as a configuration change rather than a code change within the KMA **(Req't: S46)**.

These additional links may require bi-directional signing, the signing party at each end of the link having a different private key. Different physical locations must use different signing keys **(Req't: S17).** However, it is a matter of individual risk analysis whether it is acceptable to use the same signing key over multiple logical links from the same physical platform (it is expected that in most cases such a multiple use of a signing key would be acceptable) **(Req't: S47)**.

Any private key used for signing backup versions of live data must not be accepted by verifiers except through explicit reversible management action **(Req't: S19)**

A key, unique to an individual physical link, providing traffic encryption, must be supported if the link requires it. It is a matter of individual risk analysis whether a symmetric key can be used for multiple logical links over the same physical link. **(Req't: S48)**.

The functionality surrounding the management of key material (reminders, reporting, key generation and issuance etc.) must be the same for all FTMS links, allowances being made for the different types of protection provided **(Req't: S49)**.

## 2.18 Belfast Key

### 2.18.1 Overview

Operational control of ICL Pathway central site machines is performed from a CFM site in Belfast. This link is protected by Rambutan hardware-level encryption, see Section 2.8.

## 2.19 POCL HAPS

### 2.19.1 Overview

The link between ICL Pathway and the Host Automated Payments System (HAPS) is an interim solution, whereby all AP data is sent to an existing POCL Tandem system sited at Farnborough. This HAPS system is then responsible for onward routing the data to their AP clients.

This file transfer product runs on a dedicated ICL Pathway Windows NT platform at each campus and POCL's Tandem AP Host. Windows NT platforms are used, rather than Sequent, to avoid adding complexity to the Sequent systems.

Confidentiality and integrity protection is provided for this POCL Farnborough link using Rambutan based encryption hardware. See Section 2.8 for details of handling of Rambutan keys.

This will be superseded by full links to POCL AP clients using FTP Keys over time - see Section 2.15.

## 2.20 KMA Key

### 2.20.1 Overview

In order to support the requirement stated in Section 5.1.2 there needs to be a key to encrypt data transferred between different instances of the KMC server. A key is also required to protect sensitive traffic between the KM Workstation and the KMC server. The KMA key is used for this. The KMA key is not a business-related key, but one anticipated as part of the final solution and is identified here only for completeness.

### 2.20.2 Background

The approach taken is to mirror the KMC server database across the two sites, data traffic between the sites being automatically created via the database replication mechanism. Key material held on the database is encrypted using the KMA key, a Red Pike Symmetric key. This has the effect that the traffic of key material between the sites is encrypted.

### 2.20.3 Key Management at R1c

- Not used at R1c

### 2.20.4 Key Management Requirement

NR2

1. As necessary to support other requirements.

NR2+:

2. As necessary to support other requirements.

### 2.20.5 KMA Key characteristics summary

| | KMA Key |
|---|---|
| Key Type | Red Pike Symmetric |
| Key Size | 64 bits |
| No of Concurrent Keys | 1 |
| Number of managed copies | 3 |
| Record Copies | none |
| Managed key clients | The two KMC servers and the KM workstation. |
| Boot-up Copies | none |
| Frequency of Change | yearly |

## 2.21 Key Material Specific to Siemens Metering and other Counter Applications

### 2.21.1 Overview

The KM system must be extensible, via incremental development, to support delivery of key material used by future counter applications to post offices supporting those applications **(Req't: S50)**. Some of this material must be able to be held on the PMMC **(Req't: S51)**. The nature and purpose of this key material will remain invisible to the key management code. Keys to encrypt confidential code and data associated with these applications need to be able to be supported **(Req't: S52)**

In NR2+ there is only one such application, an APS related application that has been dubbed the Siemens Metering application.

Siemens Metering Limited also require that the confidentiality of the functionality of their application software is preserved.

### 2.21.2 Background

The approach that is to be taken is twofold:

- to provide functionality to encrypt the Siemens Metering software on receipt from Siemens Metering and to decrypt it only at its destination prior to installation in FEK protected filestore. The single key used for this is called GDK. The key management system distributes GDK to post offices along the automatic channel.
- to offer general functionality to transfer counter application key material over either the interactive channel, the automatic channel or both in a manner that is as far application independent as possible. In the case of Siemens Metering, there are two separately transmitted components: DLLKA (sent over the interactive channel) and DLLKB (sent over the automatic channel). These are combined together on each post office PC to create a DLLEK value.

| | Siemens Metering Keys |
|---|---|
| Key Type | Red Pike Symmetric (GDK only). The usage of other keys is not known to ICL ICL Pathway. |
| Key Size | 64 bits (GDK only) |

| | |
|---|---|
| No of Concurrent Keys | 1 GDK and 20,000 DLLKA and 20,000 DLLKB |
| Number of managed copies | 1 of each of GDK and the DLLKA/B pairs for each post office platform. one copy of GDK at the point of encryption of the Siemens Metering Software. |
| Record Copies | KMC server keeps one of each |
| Managed key clients | All post office PCs, For GDK, the platform on which Siemens Metering code is encrypted prior to delivery to the ICL Pathway distribution centre. |
| Boot-up Copies | 1 copy of DLLKA on the PMMC |
| Frequency of Change | No changes required except as a consequence of product modifications. |

### 2.21.3 Key Management Requirements

Releases 1c and NR2:

No requirement. There is no support for this key material in these releases.

NR2+

1. The requirements below are specific to Siemens Metering.
2. Siemens Metering code and data must be encrypted (using Red Pike) on receipt from Siemens Metering **(Req't: S53)**.
3. The code and data must be decrypted only on the post office PCs where it is to execute **(Req't: S54)**.
4. The key used (GDK) must be distributed encrypted to target post offices as a normal part of the key management service **(Req't: S55)**.
5. At a post office, Siemens Metering code and data encrypted under GDK must be decrypted and installed directly into to a part of filestore subject to encryption under the filestore encryption regime **(Req't: S56)**.
6. Pending its use for decryption, GDK must be held encrypted on filestore at the post office **(Req't: S57)**.
7. The DLL enabling key must be split into two parts, neither of which, by itself, will reveal it to an attacker. DLLKA and DLLKB must not both be held on a post office PC unless one of them is encrypted under a key not itself held there. The split must be different for each post office **(Req't: S58)**.
8. It must be possible to switch to a different combination of DLLKA/DLLKB for a particular post office, should the ICL Pathway Security Manager feel that this is necessary, for example due to a possible key compromise **(Req't: S21).**
9. There is no requirement for routine changes to GDK or DLLKA or DLLKB. In particular, Siemens Metering code will be encrypted once, on its introduction to Pathway. It is not expected that it will be encrypted under a different key. However, it must be possible to encrypt a later upgrade or a new release under a different key **(Req't: S59)**. It must also be possible to issue a new release of the Siemens Metering code that uses a different DLL enabling key, and for the KMA to deliver the new enabling key to post offices using the same delivery mechanism as for the old one **(Req't: S60)**. Synchronisation logic to ensure

that the different new components are compatible will be the responsibility of the Siemens Metering code itself.

10. The contractual statements relating to Key Management in [STAT] must be supported **(Req't: S61)**.

## 2.22 Integrity of Riposte Application Software in Situ

### 2.22.1 Overview

The cryptographic infrastructure supporting the integrity of Riposte application software in situ is entirely separate from the Key Management Service that is the subject of this document, and the requirements associated with Riposte software protection are not given here. The description below is provided solely for information and completeness of coverage of the full cryptographic scene.

After installation, application software on PC's must be protected against undetected changes in situ. Standard Microsoft cryptographic techniques are used for this, the public key algorithm involved being RSA with a 512 bit key size. Verification is done by Riposte infrastructure code calling Microsoft's CryptoAPI.

Microsoft has authorised Escher as an organisation that digitally sign, or can nominate other organisations to digitally sign, software that NT will verify, when asked to do so through the CryptoAPI, prior to permitting its execution.

To achieve this in the Pathway context, Microsoft's public key is used first to verify Escher's public key, then to verify code signed by Escher, or to verify code signed by Pathway after checking the validity of Pathway's public key by validating a certificate for it signed by Escher. In this last case, a chain of trust from Microsoft to Escher to Pathway is established.

So the keys involved are:

| | |
|---|---|
| Microsoft's public key | - held embedded in the NT operating system |
| Microsoft's private key | - kept securely by Microsoft |
| Escher's public key | - held in a public key certificate signed by Microsoft |
| Escher's private key | - kept securely by Escher on a hardware storage device |
| Pathway's public key | - held in a public key certificate signed by Escher |
| Pathway's private key | - held securely by Pathway at a central site |

The public key certificates are propagated to NT platforms running Riposte in persistent object Riposte messages. The signatures for protected files are also held in similar Riposte messages.

### 2.22.2 Key Management at R1c

Not used in Release 1c.

### 2.22.3 Key Management Requirement

There are no specific requirements for key lifetimes, but it is envisaged that the Pathway private key will change at intervals. No changes to the Escher or Microsoft keys are planned at present, though over the years, procedures may evolve to enable such changes.

# 3. GENERIC KEY MANAGEMENT REQUIREMENTS

## 3.1 Requirements derived from the Cryptographic Architecture [CRYPARCH]

The [CRYPARCH] document contains a philosophy of key management as well as a number of requirements relating to cryptography and key management. We have used [CRYPARCH] as the source of the requirements below. Where differences arise, this KMS Requirements document is to be taken as the more up to date and is definitive.

### 3.1.1 Key Algorithms, Sizes and Expiry Times

The software algorithms to be used are the Secure Hash Algorithm (SHA), Red Pike and the Digital Signature Algorithm (DSA) unless otherwise specified. The exceptions in NR2+ are the bought-in VPN technology, which uses 1024 bit RSA, and the Riposte based code integrity regime, which uses 512 bit RSA **(Req't: G1)**. Also, hardware units may use Rambutan for point to point bulk link encryption. The requirements below should be seen as encompassing only the keys managed by the KMA, and therefore exclude the Riposte based code integrity regime keys.

All DSA private keys must be at least 768 bits **(Req't: G2)** except CA keys, which must be at least 1024 bits (See Section 2.10.4).

Red Pike keys are by their nature, 64 bits long.

Key management processes must cater for routine key changes of all keys except CA keys on a cycle approximating to every two years **(Req't: G4)**. CA keys have a lifetime of the order of 8 years.

Certificates must contain expiry dates that are enforced **(Req't: G5)**.

Expiry and other dates must be Year 2000 compliant. UTC dates must be used **(Req't: G6)**.

### 3.1.2 Confidentiality and Integrity of key material

The confidentiality of private and secret key material must be protected at all times. In practice this means that whenever such keys are exchanged over communications links they must be encrypted. This includes delivery over the central LANs and delivery between central sites **(Req't: G7)**.

There are three permitted exceptions to this rule:

- CHAP keys, which may need to be transmitted to the central Cisco routers in clear over the Pathway campus LAN to which the router is connected. CHAP key requirements are lifted at NR2+ as CHAP protection is superseded by VPN,
- the Red Key component of Red/Black key sets. These are by their nature transmitted in clear over the link to their destination,
- the initial transient POK value, which is distributed obfuscated but not encrypted from the boot server to the post office.

The integrity of all keys, especially public keys, must also be preserved **(Req't: G8)**.

The KMA must keep track of the installation state of all of the keys under its control, and take steps to ensure that key changes are fully performed, should delays (of configurable times) occur **(Req't: G9)**. The accuracy of the record will depend on the availability to the KMC of acknowledgements from the post offices concerned (See also Bullet 5 of Section 5.1.1).

### 3.1.3 Post office closures

*3.1.3.1 Seasonal Closures*

A post office may be subject to seasonal close down for a period of e.g. six months. Key material at such post offices must be managed so that, on reopening:

1. unexpired public key certificates are available where required, prior to restarting business **(Req't: G10)**,
2. any confidential key values that are overdue for replacement are replaced **(Req't: G11)**,
3. the latest revocation notifications are applied **(Req't: G12)**.

*3.1.3.2 Permanent Closures*

A post office may close down permanently. This give rise to the following requirements:

1. When informed of a permanent post office closure, the KMA must cause the confidential key values (in particular the POK, AP signing key and VPN private key) held at the post office to be invalidated, from the point in time requested **(Req't: G13)**.
2. When informed of a permanent post office closure, the KMA must remove the post office from its operational database, refusing to recognise it as a post office, and not scheduling further key deliveries to it, from the point in time requested **(Req't: G14)**.

### 3.1.4 Key compromise

If a key compromise is suspected, it must be possible to take immediate steps to change to new values and make the old values unusable **(Req't: G15)**. It must also be possible for such revocation not to be done immediately **(Req't: G16)**. This is so that the operational costs of early revocation can be balanced against the security risk of late revocation according to security policy.

### 3.1.5 Recovery from lost PO authentication data

Postmasters will from time to time lose the information necessary to boot up existing or install new PCs in the post office. The system must to be able to recover quickly from these situations **(Req't: G17)**.

### 3.1.6 Poor maintenance of current crypto state by postmasters

Although new key material will from time to time be transmitted to post offices, it may happen that the postmaster is slow to actually activate the new keys. A mixed key situation may arise. Normal working and recovery procedures must cater for this **(Req't: G18)**.

It is required that a key change is enforced as far as possible, short of preventing normal post office business, by stimulating the postmaster to take the necessary actions to enable the key change **(Req't: G19)**.

See also Section 5.1.1.

### 3.1.7 Application-specific security requirements

Provision must be made for cryptographic key material for counter applications to be transmitted to the post office from the KMC server and processed in post office PCs.

The application code itself may contain security information whose integrity and confidentiality must be protected en route to the post office PCs

See Section 2.21 for specific requirements.

## 3.2 Requirements arising from the Pathway Access Control Policy

The requirements below have been adapted from policy statements in [ACCPOL]. However, where a requirement also duplicates one drawn from [CRYPARCH] it is not repeated here.

1. Confidential key material (symmetric keys, DSA private keys) should be held in clear only when in physically secure environments **(Req't: G20)**.
2. Public keys (except the CA public key) should be held in certificates signed by the Certification Authority (R2+) **(Req't: G21)**.
3. Symmetric keys should only be stored on filestore where necessary. Access to such keys should be confined according to [ACCPOL] **(Req't: G22)**.
4. Part keys held in filestore must be in separate filestore **(Req't: G23)**. Access to such keys should be confined according to [ACCPOL] **(Req't: G24)**.
5. New Key Encryption Keys should not be distributed solely under the protection of existing key encryption keys **(Req't: G25)**.
6. Where a key is delivered in two parts (e.g. a red key and a black key), the parts should be delivered by different routes **(Req't: G26)**.
7. A key (or part key) that is handled manually must be held in a locked safe when not in use **(Req't: P2)**. Access to this must be authorised and recorded in conformance with Pathway procedures **(Req't: P3)**.

## 3.3 Key Generation

There is a requirement that from NR2 onwards, all central key generation be performed with the help of the hardware random number generator, unless obtained from CESG **(Req't: G29)**.

## 3.4 Automated Key Records

At Release 1c key generation is recorded manually in Excel spreadsheet/paper key record logs. For every key produced, the Key Production Log records the date and time of production, a unique identifier for the key, the algorithm (e.g. DSA), description (e.g. PA signature), number of copies issued, how issued (including label details of physical media), when issued and to whom.

Entries for CAPS Link keys also include details of the retention period used, and the previous key.

The key production log is used to record the delivery of keys and their Ids so that unique tags can be assigned to each key and template.

The key production log is maintained (manually) using an Excel workbook with a separate work sheet for each Key type (PA, SI, CAPS etc.).

There is a requirement that this be automated so that key generation logs become automatically created in a suitable electronic form, rather than paper-based **(Req't: G30)**. It must be possible for relevant parts of the log to be updated, but this should be controlled and policed **(Req't: G31)**.

## 3.5 Certification Authority Workstation

It is required in NR2+ to have a Certification Authority Workstation (CAW) with the following characteristics:

1. Any network to which the CAW is connected must be private, dedicated solely to the CAW's functions and must be physically secure. **(Req't: S62)**.

2. The CAW must be positioned in a highly secure area, with access restricted as agreed by the Cryptographic Key Manager **(Req't: S63)**
3. The CAW must only be capable of operation when a CA private key has been loaded onto it **(Req't: S64)**
4. The CA private key must be loaded onto the CAW in 2 parts by staff using two different roles **(Req't: S65)**
5. No individual should know the whole CA private key **(Req't: S66)**.
6. The CAW will be capable of receiving uncertified public keys on a suitable removable media - e.g. floppy disk. It should be possible to present these in batches as well as singly **(Req't: S67)**.
7. Will be capable of signing a public key (or batch of public keys) using the CA private key, producing certificate(s) containing the signed public key(s) **(Req't: S68)**.
8. The certificate semantics will be based on X.509 standards, but need not be fully X.509 conformant **(Req't: S69)**.
9. The mechanism must allow the certificates to be generated with a defined date after which the certificate is not valid (based on validity of CA keys and the validity of the private key corresponding to the certified public key) **(Req't: S70)**. This must be tailorable by the CA **(Req't: S71)**.
10. The CAW will be capable of writing the certificates to removable media **(Req't: S72)**.
11. The CAW must be capable of signing (batches of) revocation messages **(Req't: S73)**.
12. The CAW must require authentication that includes a physical authentication token or is of similar authentication quality **(Req't: S74)**.
13. The CAW must time out if not used for a period of time, requiring re-authentication for re-use **(Req't: S75)**
14. Availability and performance - see Sections 5.1.4 and 5.1.5.

*Note:* *It is Barry's call whether requirement 2 above makes requirement 12 unnecessary (12 is not currently planned to be satisfied). However, despite physical security considerations, I still believe that 12 *should* be a requirement. Password authentication is not in my view appropriate for a sensitive service like this one.*

## 3.6 Security Event Management

There are three general requirements:

- [SFS] conformant and SEM conformant auditing (elaborated below) and event logging to NT event logs must be supported **(Req't: G32)**.
- No plain-text key values must appear in audit logs **(Req't: G33)**.
- Security copies of old key values must be kept in a physically secure place in case they are subsequently needed for legal or audit investigations **(Req't: P4)**.

CAW events are handled outside the scope of SEM, so separate facilities must be provided for viewing and printing off CAW logs **(Req't: S76)**.

This rest of this section expands on what is meant by SEM conformant auditing/event mgt.

The [SEM] highlights a number of major areas for consideration. These are:

1. User administration (log on/off, timed)
2. Security incidents
3. System administration events
4. Administration logs
5. Network Mgt logs
6. Supporting events
7. Specific security events (e.g. key mgt)
8. Configuration events (e.g. KMC server switch-over)

View access must be logged as well as update access.

Riposte messages should be logged (note happens automatically)

In terms of Key Management this is understood to mean that the events required to be logged are:

**General**

- System start-up
- System restart
- Controlled System Shutdown

**KMA**

- logon/out, success and failed attempts
- Prompts and nags
- Key change requests
- Key change confirmations
- Receipts of FAD data
- Key change activities in sequence, including key cancellation and key requests
- Loading of Key data
- Key creation events

- Key packages sent out
- PO sign-in
- PO recovery
- Help desk activities
- Viewing of keys
- Changes to key time-outs
- Certificates requested and sent out
- D-H exchanges (stage by stage)
- Revocation messages (in and out)
- Any Security Failures
- APP-specific material generation or receipt

**Post offices**

- Key packages arriving, and actions taken as a result
- Signing of a message
- Verifying a key
- Any security fails
- Moving to new key
- Revocation Messages and actions taken
- All stages of key change processes
- PIN Changes
- Recovery process - stage by stage

**Key Generators**

- Key creation
- Key records

**CA Workstation**

- Logon/logoff, success and fails.
- Keys Received
- Key certification
- Certificates extracted
- Revocation message certification

VPN Servers

- Administrator logon/logoff, success and fails
- Policy, Configuration and Key file changes
- PIN submissions, good and bad
- Session key establishment failures (except “encrypt if you can”)
- VPN community member authentication failures

**Verifiers (on campus)**

- Security fails

- Events for handling public key material

**Help Desk**

- Recovery requests and action taken
- Postmaster verbal authentication successes and failures

**Other (e.g. CAPS machines)**

- Key changes (both ends)

# 4. SOCIAL SYSTEM

This section contains a summary of pertinent factors of the organisational and people-based operations of the Pathway system. It looks at the business processes being operated in the work groups, in order to bring out the effects on the requirements for key management, and way that key management may affect them.

At Release 1c we observed that a large proportion of problems arose from mismatches between the solution and the social system into which it was to fit. This section attempts to address this in order to reduce the number of such problems.

## 4.1 Day to Day Site Operations

### 4.1.1 Background

Where a non-post office site hosts an NT platform that uses a private key, the value is sent encrypted over the automatic channel using Riposte, the encryption key for it being sent separately on an externally presented exchangeable medium. Although these machines are managed from one remote CFM site, there are on-site CFM operations staff looking after the day-to-day functions that cannot be managed remotely. The physical loading of the key encryption key, on booting up a machine, is one of those functions.

There are separate administration arrangements for BA, PAS and DLR remote machines. It is assumed that similar functions are performed at all of these sites, and that the staff involved will have broadly the same access rights to the systems they are managing.

In the event of a system break of any kind, there are penalty clauses, which apply if a machine cannot be brought back up within a pre-determined period of time. On some sites, recovery time-scale requirements are too short to be able to depend on any off-site staff being brought in to perform the restart. People on-site are generally network people - the only local operational role. They are not vetted security staff. On other sites, ones that have only one Pathway PC on them, CFM may bring in external support to re-boot a broken PC. However that individual will also be a network support person.

If a fault requires replacement of a PC, current policy is to have a replacement permanently available on the site of the PC it is to replace. There is a general requirement to keep the software on this backup machine up to date. This cannot be done as a special exercise, downloading all Tivoli updates when it is brought into service, because the CFM contract with Tivoli is for downloads to be available only in working hours, and breakdowns can occur at any time. This means that updates both to the live PC and the backup must be done at the same time, and consequently that the backup PC must be powered on and linked to the Tivoli delivery network alongside the live PC, even though it will not otherwise be operational. The consequence of this is that encrypted keys delivered via Riposte as part of a key change, will be able to be transmitted to the backup PC at the same time as to the live PC.

Once the backup PC has been swapped in, a new, factory fresh backup will need to be brought in and brought up to date as soon as possible.

[ACCPOL] defines the following Access Control Policy roles for administering cryptographic key material:

| Role | Main functions |
|---|---|
| Cryptographic Key Manager | Generating or obtaining cryptographic keys and organising their distribution. |
| Cryptographic Key Custodian | Initial installation of cryptographic keys where this needs to be done manually. Periodic update of these keys. |
| Cryptographic Key Handler | Handling the part of a cryptographic key that is held on an exchangeable medium when this needs to be re-installed e.g. when a system is rebooted. |

The requirements that follow are expressed in terms of these roles. [ACCPOL] also defines the role of ***PO Key Recoverer***. This role, used primarily by the Help Desk, is discussed in Sections 4.5 and 4.7.

### 4.1.2 Requirements

It must be possible for an operational staff member already on shift to (re-) boot an on-site machine without having to call in external support. This means that on the affected sites, the person needs to be sufficiently trusted and given sufficient access rights to take on the role of Cryptographic Key Handler, a role which has access to the required part key, held in a key safe **(Req't: P5)**.

It must be possible for a Key Handler to be able to boot up a backup PC that is replacing a broken one. This means that whenever a Key Custodian visits the site to install a new key, it must also be installed in the backup PC so the two machines are in synch. It also means that the backup's Riposte service must have been run up, with the backup PC on line, sufficiently recently to have received the latest automatic channel key component **(Req't: G36)**.

These people do not have, and must not need to be given, access to privileged logons (e.g. root) to perform their duties, so the cryptographic aspects of boot-up must not require such access **(Req't: S23)**.

Also, because of the lack of security clearance of the individuals involved, an exchangeable medium containing key material must be of no use, by itself, to an attacker. In practice this means that it should contain only a key part, not the full in-clear key **(Req't: G37)**.

## 4.2 System Management

System management actions should not require any access to key material **(Req't: G38)**. However:

- if a system management action requires a platform to be rebooted, the requirements relating to speed of completing a re-boot, described in the previous sub-section, need to be considered **(Req't: G39)**,
- if a system management action results in the replacement of a machine, the security management actions relating to the initial installation of key material need to be able to be performed. When a new NT platform is installed to replace a broken one, Key Custodian privileges will be required to initialise the machine with the current or replacement key values **(Req't: G40)**. In particular it must be possible for a key part to be transmitted down the communications link and installed on the machine within the contracted time allowed for restoring service on that link **(Req't: G41)**.

- old key material held on filestore of discarded equipment must be destroyed, or rendered valueless (for example by destruction of a key's exchangeable medium component, or by revocation in the case of a private key), or must continue to be physically protected after equipment removal **(Req't: P6)**.

## 4.3 Network Management

It is in relation to VPN that security requirements arise:

In NR2+, VPN policy files need to be set up and maintained with the correct IP addresses and security settings.

Router settings, which ensure traffic passes through the appropriate VPN Servers, both inbound to the campuses and outbound from them, must be securely managed. Their integrity is a security issue, though not a key management requirement.

The VPN security regime must be able to recover from any communications breakdown that the regime may erroneously cause, in particular through errors in key management, within time-scales conformant to network serviceability commitments. See Section 2.4 for specific requirements.

## 4.4 Security Management

Key management is a part of security management in general. [ACCPOL] separates key management duties into three main roles: Creation of new key material, done by the Pathway Key Manager, installation of new key material, done by a Key Custodian, and re-activation of key material, done by a Key Handler. Key Handler actions are also covered separately in Section 4.1.

The following technical requirements apply to controls over the administrative processes used to perform routine key installation and changes:

- Separation of duty: the Key Handler role must not be able to create (using Pathway facilities) or install a new key value **(Req't: G42)**.; the Key Custodian role must not be expected to boot up a system and should not be able to create new key values **(Req't: G43)**.; the Pathway Key Manager role should not be able to manually install values he or she has created, or re-boot an operational business system **(Req't: G3)**. This does not mean to say however, that a suitably vetted individual may not be given multiple roles should operational conditions require it.
- The Key Custodian role should not need to have privileged access to the system on which he or she is installing a key, except to perform the specific installation function itself **(Req't: G44)**. No actions unrelated to key installation and review should be available to the Key Custodian role **(Req't: G45)**.
- Routine key changes must be possible without the intervention of anyone other than the Key Custodian **(Req't: G46)**.

Alarm and Alert handling will depend on the general security event solution.

## 4.5 Configuration Management

Software distribution is done from CM at Feltham. The Key Management solution must be able to support the distribution and ongoing maintenance of SI signing key material for this site **(Req't: S77)**.

Auto-config is currently controlled by the implementation unit at Feltham, but there are suggestions that the process may move to the data centres (Wigan and Bootle). Some of the data downloaded to a post office at rollout time is signed using the SI signing key. The Key Management solution must therefore be able to support the distribution and ongoing maintenance of SI signing key material for these sites, keeping these two and the Feltham sites sufficiently synchronised so that valid signed messages from all three sites will always be accepted at post offices and other target systems, even though the different sites may transiently be using different signing keys **(Req't: S78)**.

Before NR2+, Initial CHAP key values are distributed from the implementation unit. The medium on which they are stored was required to remain physically secure and backed up at all times. Whenever a post office gateway PC is swapped out, it was primed with a new copy of the current CHAP key for that post office.

The role that can ask for the new CHAP key has not been defined in [ACCPOL] but a suitable one would be ***PO Key Recoverer***. However if procedures in the implementation unit are such that too many staff would be given this role (remembering that it is also empowered to recover post office filestore key values), then it would be better to devolve this access privilege to one of the support engineer roles associated with rollout.

There is an overlap here with the requirements of the next section.

## 4.6 Manufacturing and Logistics

Manufacturing produce PC's tailored to a pre-defined configuration. All Gateway PC's are produced to the same configuration. This configuration can be tailored by CM (Tivoli) at installation time. At the same time, installed key sets and any revocation information that may be extant need to be able to be brought up to date before the PC is used for business transactions. This involves Tivoli at autoconfig time (and at other times up to and including NR2, superseded by Riposte messages from the KMC server in later releases). In NR2+, the current VPN Keys (both normal and exception) need to be sent to the post office. The key value is obtained from the KMC server.

Post office installation is performed by installation engineers, who do not have the expertise to diagnose installation problems. They are instructed to swap in a new PC if an installation fails. The VPN key delivery process must not prevent a restart of the installation process on the new PC **(Req't: S82)**.

## 4.7 Help Desk

Help desks are located in Stevenage and Manchester. They help support the recovery of key material lost from post offices. Only individuals permitted to play the ***PO Key Recoverer*** role should be able to provide or initiate the provision by the KMC server of recovery key material **(Req't: G47)**. When the KMA is implemented this will involve a Communication between the Help Desk and the KMC server. The link used for this must be integrity protected to prevent false authorisations by wiretap **(Req't: S83)**. The help desk individual must be authenticated and individually accountable for actions taken **(Req't: S84)**.

# 5. PERSPECTIVES

This section expresses the requirements from the perspective of each 'user' of Key Management. The term 'user' is used in a broad sense meaning all those parties with any interest in key management, and its implementation in Pathway, not just the people who will be using it.

The perspectives are subdivided into aspects, some of which are common across perspectives. The aggregation across the perspectives gives a requirement set for each aspect.

## 5.1 Key Manager Perspective

### 5.1.1 Functionality

1. Viewing of key information including key period (but not key value) must be possible, including when a key went into service and when it due to be replaced **(Req't: G48)**.
2. Updating of key periods must be possible **(Req't: G49)**.
3. For keys whose management is not fully automatic, the system must prompt a month in advance of key change being due **(Req't: G50)**, and then, until the key change is confirmed complete, again on the day the key change is due **(Req't: G51)** and daily thereafter **(Req't: G52)**.
4. Post Office-specific keys should be changed without prompting the ICL Pathway Key manager (e.g. POK, FEK, VPN, and AP), but it should still be possible to instigate a change manually, and to control the process manually - e.g. to mark a PO to be excluded **(Req't: G53)**.
5. The KMC must be kept informed by a post office of which keys have been installed on which platforms at that post office **(Req't: G54)**.
6. Failure to receive notification of installation within a policy defined period must be able to be alerted to the Pathway Key Manager **(Req't: G55)**.
7. It must be technically possible to replace any key on a regular periodic basis, or rapidly on compromise **(Req't: G56)**.
8. Key management should be as automated as possible **(Req't: H8)**.
9. Where keys are to be kept off-line they should be kept on floppy disks or memory cards or CD-ROM, with non-removable labels **(Req't: G57)**.
10. Floppy disks should be duplicated for resilience purposes, but kept together at all times **(Req't: P7)**.
11. Instigation of key part distribution over the wire via the KMC server must be supported **(Req't: G58)**.
12. Confirmation of key changes are required **(Req't: G59)**.
13. The link between the Key Manager's workstation and the KMC server needs to be a high security one with mutual authentication **(Req't: S85)**. Particularly sensitive operations and data transferred across that link must be cryptographically protected **(Req't: S86)**.

See also the requirements relating to the CA keys in Section 2.10.4.

### 5.1.2 Security

1. The CAW must be off-line at all times in a secure location with access restricted **(Req't: S87)**.

2. The CAW must time out if not used for a period of time, requiring re-authentication for re-use **(Req't: S36)**.
3. From NR2+ onwards, all public keys except the CA's itself must be protected in a certificate signed by the CA **(Req't: G60)**.
4. Suspected compromised keys should be able to be revoked immediately to prevent their exploitation, though revocation must be able to be delayed by explicit decision of the Key Manager to take the business risk on the grounds that immediate revocation would be more costly. See Section 3.1.4.
5. Keys should only be stored where necessary, and be held securely **(Req't: G61)**.
6. No human being should need to see any confidential operational key value **(Req't: G62)**.
7. Where a key is delivered in 2 parts (e.g. red key black key) the parts should be delivered by different logical routes (e.g. one over the automatic channel and one over the interactive channel) **(Req't: G63)**.
8. A key should not be online until it is due to be used, or shortly before, since expiry is considered to start at that point in time (except public keys) **(Req't: G64)**.
9. Post office FEK, POK, VPN and APPR Keys should be replaced at a Post Office, by a routine, automated key refreshment procedure, at intervals agreed with the Contracting Authorities, based on advice from CESG **(Req't: G65)**.
10. Any key material passed between the Pathway campuses must be encrypted under Red Pike using a key shared between the KMC servers at each campus **(Req't: G66)**.
11. From NR2+ onwards, the KMC server will be the source of the FEKs for all files except the swap file, for which a new key will be dynamically established on each PC on each boot-up **(Req't: S41)**.

### 5.1.3 Auditability

See Section 3.6.

### 5.1.4 Performance

1. Must cater for rollout rates (300/week) alongside migration of NR2 post offices (at a similar rate) and routine key changes to already installed NR2+ post offices **(Req't: G67)**.

### 5.1.5 Availability

1. The KMA functionality should be available to the key manager located in FEL01, with controls over access and protection of key material that are broadly as strong as for management access from within the ICL Pathway campus **(Req't: S42)**.

### 5.1.6 Migration

1. A mechanism must be defined to enable existing post offices to be moved smoothly onto NR2+ key management mechanisms without loss of security **(Req't: G68)**.
2. Migration must be possible from NR2 PO's **(Req't: G69)**.
3. Migration must not require visiting the PO except in rare situations **(Req't: G70)**.
4. The key management aspects of migration of a PO must not cause more than the contracted loss of service, broadly this is 4 hours for a non-operational PO and 8 hours for a PO in degraded mode. The definitive text can be found in [G10] **(Req't: G71)**.

5. Routine migration of a post office to NR2+ (using VPN) from NR2 (using CHAP) must not require manual synchronisation of VPN encryption policy file information on every migrated post office. Manual synchronisation should be required only in exception situations **(Req't: G72)**.

### 5.1.7 Usability

1. A modern Key Manager GUI for normal operational activities must be provided **(Req't: G73)**.

### 5.1.8 Reliability

1. Resilience to Key Manager finger trouble is required **(Req't: G74)**.
2. The ability to reset to a consistent state, so that communications can continue and subsequent recovery is possible, if a communications or other failure cause a key mismatch during a key change protocol **(Req't: G75)**.

## 5.2 Key Custodian Perspective

### 5.2.1 Functionality

1. Must be able to install and activate a new key at each site that is using part key material from exchangeable medium in conjunction with matched values present on the system **(Req't: G76)**.
2. Must be able to confirm that a key change attempted has been correctly achieved **(Req't: G77)**.

### 5.2.2 Security

1. Secure storage is required, of part key material on exchangeable medium on all sites at which the Key Custodian operates **(Req't: G78)**.

### 5.2.3 Auditability

1. [SFS]-conformant and SEM-conformant event logging to NT event logs. See Section 3.6.

### 5.2.4 Availability

1. Reinstallation of a lost key must be possible at all times that the system is operational **(Req't: G79)**.

### 5.2.5 Usability

1. A modern Key Custodian GUI for normal operational activities must be provided **(Req't: G80)**.

### 5.2.6 Reliability

1. Resilience to Key Custodian finger trouble is required **(Req't: G81)**.

## 5.3 Key Handler perspective

### 5.3.1 Functionality

1. Ability to obtain the necessary exchangeable medium to boot up systems on the sites the key handler operates on **(Req't: G82)**.
2. Notification if the key in use is causing communications failures **(Req't: G83)**.

### 5.3.2 Security

1. Secure storage of part key material on exchangeable medium on all sites at which the Key Handler operates **(Req't: P8)**.

### 5.3.3 Auditability

1. [SFS]-conformant and SEM-conformant event logging to NT event logs. See Section 3.6.

### 5.3.4 Availability

1. Reboot must be possible at all times that the system is required to be operational **(Req't: G85)**.

### 5.3.5 Usability

1. A modern Key Handler GUI for normal operational activities must be provided **(Req't: G86)**.

### 5.3.6 Reliability

1. Resilience to Key Handler finger trouble is required **(Req't: G87)**.

## 5.4 Certification Authority Perspective

### 5.4.1 Security

- as Section 5.1.2
- a broken CAW should be kept physically secure until confidential key material on its filestore can be erased **(Req't: S43)**.

### 5.4.2 Performance

1. CAW must be capable of coping with flow of certificates (average 300/week), and a sudden rush of 20,000 over a two day period (in case a CA key is compromised) **(Req't: G88)**.

### 5.4.3 Availability

Since the KM workstation is used to prepare material for on the exchangeable medium that is used to pass key material to and from the CAW, the CAW availability requirements extend to the KM workstation.

1. In the event of a software failure, the CA, comprising in this context the CAW and the KM workstation should be recoverable and able to issue revocations within one hour **(Req't: S45)**.
2. In the event of a hard CAW hardware failure, it should be possible to have the CAW running on an alternative machine on the same site within 12 hours. In this case, the Pathway Key Manager may choose to visit the CA on the other Pathway site in order to obtain quicker service **(Req't: S79)**.
3. In the event of a hard KM workstation failure, a substitute should be made available on the same site within 12 hours **(Req't: S80)**.

## 5.5 Data Centre Operator Perspective

### 5.5.1 Usability

1. Key management must not require data centre staff not responsible for key handling to have any knowledge of it **(Req't: H9)**.

## 5.6 Key Holder Perspective (Data centre and elsewhere)

### 5.6.1 Security

1. Keys must be held securely by the holder **(Req't: P9)**.

### 5.6.2 Usability

1. Keys must only be requested when absolutely needed (boot up and key change) **(Req't: G90)**.
2. Keys must never need to be asked for before the key holder has received them **(Req't: G91)**.

## 5.7 Security Auditor Perspective

### 5.7.1 Functionality

1. All security events must be logged (as per [SEM]). See Section 3.6.
2. Must be able to review underlying key data (e.g. status of keys but not their values) **(Req't: G92)**.
3. Requires access to audit information (even off-line servers) **(Req't: G93)**.

## 5.8 External Post Office Auditor/Emergency Manager Perspective

### 5.8.1 Functionality

1. Requires features to examine PO key statistics **(Req't: G94)**.
2. Needs ability to get PO keys (specifically POK, FEK, and APPR) changed from the centre **(Req't: G95)**.
3. Needs to be sure that nobody else can do this of their own accord **(Req't: G96)**.
4. Needs the ability to review audit logs **(Req't: G97)**.

## 5.9 Post Office Engineer Perspective

### 5.9.1 Usability

1. Must not require specialised knowledge of key handling **(Req't: H10)**.
2. Must be possible to install a replacement PC and get it serviceable in 30 minutes **(Req't: G98)**.

## 5.10 Post Office Manager Perspective

### 5.10.1 Usability

1. Automatic recovery from loss of PMMC or PIN (via help desk phone call) **(Req't: S81)**, even if the post office is not on-line **(Req't: 88)**.
2. The procedure must be simple and well defined, not requiring any IT knowledge **(Req't: S89)**.
3. Routine key change procedures should be simple and well defined **(Req't: H11)**.

### 5.10.2 Reliability

1. Key mgt must not cause loss of service during opening hours **(Req't: H12)**.

### 5.10.3 Performance

No special requirements identified.

## 5.11 Post Office Staff and Customers Perspective

### 5.11.1 Usability

1. Key mgt should be totally invisible to these people (other than seeing the PMMC inserted at boot-up by the postmaster) **(Req't: H13)**.

## 5.12 Post Office Trainee Perspective

### 5.12.1 Security

1. Training mode working at a post office must not compromise the security of operational keys **(Req't: G99)**.
2. Training mode working at a post office must not compromise the cryptographic protection provided by operational keys for operational data **(Req't: G100)**.

## 5.13 Help Desk Operator Perspective

### 5.13.1 Functionality

1. A help desk operator must be able to tell KMC server that a PO needs recovering **(Req't: S90)**.
2. A help desk operator needs to be able to authenticate a postmaster over a remote voice link (telephone line) **(Req't: S91)**.

### 5.13.2 Availability

None

### 5.13.3 Usability

1. A simple GUI is required for the Help Desk Operator - giving access only to authorised functions **(Req't: S92)**.

## 5.14 Enterprise Mgt Perspective (ICL Pathway and POCL)

### 5.14.1 Security

1. All asymmetric keys must be revocable within hours rather than days **(Req't: G101)**,
2. Asymmetric keys should be made to expire through the use of certificate expiry dates, but to prevent loss of service through late scheduled key changes, warnings for key types whose refreshment is not fully automatic must be issued to the Pathway Key Manager for a policy defined period prior to expiry. See Section 5.1.1.
3. the requirements of the Pathway access control policy [ACCPOL] must be met in terms of:
   - logon procedures, for remote help desk and for key manager **(Req't: G102)**.
   - accountability **(Req't: G103)**.

### 5.14.2 Reliability

1. Lack of reliability should not prevent the service from satisfying availability requirements expressed elsewhere in this document **(Req't: H14)**.

### 5.14.3 Availability

1. Changes of operational business keys should not require reboots of machines, but may require reboots of Riposte Desktops **(Req't: G104)**.
2. If a change to a key protection key is done via exchangeable medium, a reboot is acceptable, but this must be able to be done at a time chosen by the local Key Custodian to minimise business impact **(Req't: G105)**.
3. Except in a rollout situation, unavailability of the KMC must not prevent a post office from doing business **(Req't: G106)**.

### 5.14.4 Auditability

See Section 3.6.

### 5.14.5 Potential for Change

1. The KM service must be extensible to cope with mgt of key material for post offices that is specific to particular counter applications, without knowledge of the internal structure of that key material. See Section 2.21.
2. It must be flexible to cope with as yet undefined new symmetric and asymmetric key material and its transmission, without changing the basic architecture the KMA **(Req't: G107)**.
3. It must be flexible to cope with additional instances of clients for existing key types (for example additional FTMS clients) where such additions are technically meaningful **(Req't: G27)**.

### 5.14.6 Migration

See Section 5.1.6.

### 5.14.7 Installation

No special requirements identified.

## 5.15 Technical Support Perspective

1. Any crypto protection provided for a pathway platform must not prevent technical support staff from doing their job. In particular, it must not prevent support staff from running any diagnostic software that current access control policy permits **(Req't: G28)**.
2. Unauthorised technical support staff should not be able to see, or otherwise obtain for future use, any key material that is continuing to provide protection for operational data **(Req't: G34)**. In some cases, it may be necessary for support staff to physically remove a platform from its operational position. This should not compromise this requirement **(Req't: G35)**.
3. Support staff must be provided with enough information for problems arising from key management related incidents to be accurately identified and fixed **(Req't: G84)**.

## 5.16 Application Developer Perspective

1. The key management system must be developed with a level of development security consistent with good practice **(Req't: G89)**.
2. Live confidential key values must not be used in the testing environment **(Req't: G108)**.

# 6. APPENDIX A: SUMMARY OF KEY USAGE

The following table is a matrix of keys and destinations (managed key clients) in NR2+. A tick shows that the key in that column must be distributed to the platform on that row.

| **Managed Key** | AP | | SI | | PA | | CA | FEK | POK | VPN | KI | CAPS | CMS | TIP/RD | | AP Client | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Client** | Pr | PKC | Pr | PKC | Pr | PKC | Pu | | | | Pu | | | Pr | PKC | Pr | PKC |
| Post office gateway PC | ✓ | | | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | |
| Post office secondary PC | ✓ | | | ✓ | | ✓ | ✓ | ✓ | | | ✓ | | | | | | |
| AP harvester | | ✓ | | ✓ | | | ✓ | | | | | | | | | | |
| CM signing server | | | ✓ | | | | | | | | | | | | | | |
| BPS loader agents | | | | ✓ | ✓ | | ✓ | | | | | | | | | | |
| Vector server | | | | ✓ | ✓ | | ✓ | | | | | | | | | | |
| Central VPN Security Servers | | | | ✓ | | | | | | ✓ | | | | | | | |
| CAS VME platform | | | | | | | | | | | | ✓ | | | | | |
| CAS Oracle db platform | | | | ✓ | | | ✓ | | | | | ✓ | | | | | |
| TIP/RD Pathway gateway | | | | ✓ | | | ✓ | | | | | | | ✓ | ✓ | | |
| TIP/RD POCL gateway | | | | ✓ | | | ✓ | | | | | | | ✓ | ✓ | | |
| RD POCL gateway | | | | ✓ | | | ✓ | | | | | | | | | | |
| POCL Client sites | | | | ✓ | | | ✓ | | | | | | | | | | |
| POCL Client Gateway | | | | ✓ | | | ✓ | | | | | | | | | ✓ | ✓ |
| CMS local gateway | | | | ✓ | | | ✓ | | | | | | ✓ | | | | |
| CMS remote gateway | | | | ✓ | | | ✓ | | | | | | ✓ | | | | |
| All other Tivoli-managed | | | | ✓ | | | ✓ | | | | | | | | | | |

Rambutan key values and the CK key are not shown as they are not managed by the key distribution service (though in the case of Rambutan, reminders for key changes are supported by the KMA).

It will be seen that two keys, the SI public key certificate and the CA public key, must be distributed to many different types of client. It will also be seen that the post office workstations (gateway and secondary) receive many different keys.