

RFID Weapons and Armoury Management System

Publication No. 25/06

Applying the technology to an armoury application and description of a Case Study



G Dean

RFID Weapons and Armoury Management System

Applying the technology to an armoury application
and description of a Case Study

G Dean

Publication No. 25/06

1.0

RFID Weapons and Armoury Management System

Applying the technology to an armoury application and description of a Case Study

G Dean

Publication No. 25/06

1.0

FIRST PUBLISHED MAY 2006

© CROWN COPYRIGHT 2006

The text of this publication may not be reproduced, nor may talks or lectures based on material contained within the document be given, without the written consent of the Director, Home Office Scientific Development Branch.

Home Office Scientific Development Branch
Sandridge
St Albans
AL4 9HQ
United Kingdom

Telephone: +44 (0)1727 865051

Fax: +44 (0) 1727 816233

E-mail: hosdb@homeoffice.gsi.gov.uk

Website: <http://scienceandresearch.homeoffice.gov.uk/hosdb/>

Contents

	Page
Management Summary	5
1 Introduction	6
2 Part 1. Background.....	8
2.1 System requirements	9
2.2 Project objective	10
2.3 Methodology	10
2.3.1 User's operational requirements	10
2.3.2 Technical specification	11
2.3.3 Tender process	12
3 System fundamentals	13
3.1 Management computer	13
3.2 Overview of the issue process	13
3.2.1 User options – issue, return and move weapons.....	14
4 The basic principles	16
4.1 What is RFID and why use RFID in this application?	16
4.2 Identifying an authorised firearms officer (AFO)	17
4.3 Identifying a weapon	17
4.4 Weapon RFID tags.....	18
4.5 Handguns	18
4.6 Long arms	19
5 User functions.....	21
5.1 Hand-held computer user functions	21
5.2 Management computer and reports	21
5.2.1 Logging in.....	22
5.3 Access control	24
6 Technical specification - system enhancements	25
6.1 Wireless data transfer	25
6.2 Wireless system updates	26
6.3 SMS text alerts	26
7 Part 2. Case study	27
7.1 Introduction.....	27
7.2 User and operational requirements.....	27
7.3 Physical location.....	27

8	System description	29
	8.1 Firearms officers' cards.....	29
	8.2 Weapons tagged	29
	8.3 Locations.....	29
	8.4 System architecture	31
	8.4.1 Technology	31
	8.4.2 Hardware	31
	8.4.3 Hand-held computer	31
	8.4.4 Transmitting data wirelessly – externally and internally	33
	8.4.5 Desktop computer.....	33
	8.4.6 Management reports.....	33
	8.4.7 Authorisation levels – weapons issuing.....	36
	8.4.8 Unauthorised issuing	36
	8.5 Ammunition	37
9	Description of the processes - weapons issue, return, movement and administration...39	
	9.1 Weapons issue – operational.....	39
	9.2 Weapons issue – training.....	42
	9.3 Weapons issue - retrospective.....	44
	9.4 Weapons return.....	46
	9.5 Weapons movement	48
	9.6 Administration	48
10	System features	49
	10.1 Access control.....	49
	10.2 Typical system notifications	50
	10.2.1 Internal	50
	10.2.2 External SMS alerts	51
	10.3 System security.....	52
	10.4 System training	52
	10.5 Rough order of cost	53
	10.6 Benefits of the system.....	54
	10.7 Limitations	55
11	Conclusion.....	56
	11.1 Lessons learned.....	56
	11.2 Recommendations	57
	11.3 Possible future developments.....	57
	11.4 Partnership working	57
	11.5 Contact details	58
Appendix A:	The user's operational requirements	60
Appendix B:	Process flowchart – weapons issue for operational use.....	69
Appendix C:	Process flowchart – weapons issue for training.....	70

Appendix D:	Process flowchart – weapons issue retrospectively.....	71
Appendix E:	Process flowchart – weapons return	72
Appendix F:	Process flowchart – weapons movement.....	73
Appendix G:	Glossary of terms	74

Management Summary

This document describes how a partnership between the Home Office Scientific Development Branch (HOSDB) and an operational Police Firearms Support Unit has developed a showcase demonstrator of a stand-alone, computer-based weapons and armoury management system. The demonstrator system uses a range of existing technologies, including radio frequency identification (RFID) tags, as a means of identifying individual officers and weapons and recording the issue of police firearms from both fixed and mobile armouries. The project aims to determine whether it is feasible for this type of technology to meet the requirements of this particular application, and to create a pilot demonstrator system.

The project is a result of the review by the Police Complaints Authority (PCA) on shootings by police in England and Wales from 1998 to 2001. Recommendation 21 of this review states:

“ACPO should review the methods used for recording the booking out of weapons, ammunition and other firearms equipment.”

The purpose of the system is to:

- Give an immediate issue/no issue decision based on weapon type and level of officer authorisation.
- Provide quick information regarding the current location and status of a weapon.
- Provide an auditable record of all firearms issues, returns and movements.
- Provide an element of ammunition stock control and weapons maintenance information.
- Provide management information and generate reports based on real-time information, to include a full weapons inventory at any given time.

The goal of the project is to address the PCA Recommendation 21 and improve the efficiency and day-to-day management of the firearms issue information using a user-friendly computer-based system and effective use of current technology. The system introduces tighter controls on the weapons management process and the ability to produce accurate, up-to-date reports for audit trail purposes. The system capabilities also extend to controlling and monitoring access to the armoury.

1 Introduction

This two-part report contains details of the development of a stand-alone, computer-based management system for a police armoury. The system demonstrates how radio frequency identification (RFID) technology has been applied to assist in the identification of individual Firearms Officers and control and recording of the issuing of firearms. The system was developed in partnership with a Firearms Support Unit and, as the end-users, reflects their specific operational requirements which are included in Appendix A. The showcase system would be used to demonstrate how the technology was applied to meet this particular requirement. Details of how this project met each of these requirements are also included in Appendix A. The system is stand-alone and is not to be connected to the 'classified' Police IT Network.

RFID tags were securely adhered to a range of conventional operational firearms currently in use by the UK police. RFID tags were incorporated within Firearms Officers' personal identity cards. To identify Firearms Officers and firearms, the RFID tag is read electronically using a hand-held computer and this information is then transferred and verified against a computer database. The tags do not continuously transmit real time geographical location of officers or firearms. TASER® devices were not included in this project.

Part 1 outlines the user's requirement, the process that was followed to develop the system and a description of the technology used.

Part 2 describes a Case Study of a pilot showcase system developed and installed in a Firearms Support Unit at a UK police force.

This document can also help to provide information that can be used as guidance for forces planning similar developments and which may benefit from lessons learned from the project.

In Part 1:

- Chapter 3 explains why the system is needed, what the system would be required to do, the objective of the project and the early process that was followed to achieve the objective.
- Chapter 4 describes the fundamentals of the system and the options that a computer-based system makes available to the user.
- Chapter 5 outlines the basic principles of the system and how RFID technology was used in this application to identify firearms officers and weapons.
- Chapter 6 outlines the functionality of the hand-held computers, the desktop management computer and the reports that can be generated and how access control to the armoury can be integrated into the system.
- Chapter 7 describes enhancements made to the system to include wireless data transmissions updating the system, allowing weapons issue transactions to be made from Armed Response Vehicles (ARVs) or out in the field. This section also describes how SMS messaging can be sent by the system to a mobile phone as notification to specified alerts.

In Part 2:

- Chapter 8 provides an introduction for the Case Study installation of a demonstration system at a UK police force.
- Chapter 9 describes the system, the technology and the hardware used in the Case Study. This is followed by a more in-depth explanation of the hand-held computers and the desktop management computer, and describes some of the management reports that are available to print off.
- Chapter 10 summarises the processes of weapons issue, return, movement and system administration that can be carried out using the hand-held computers. Screen images of the hand-held computer show some key steps in each process. Appendices B, C, D, E and F explain in more detail the step-by-step process for each transaction in the form of flowcharts.
- Chapter 11 describes some of the features of the system, including the capability to integrate access control to the armoury, system notifications to particular events and the security levels included within the system's development. The chapter goes on to suggest approaches to training on the system and a rough order of cost of a system comparable to the Case Study installation. The chapter closes by listing the benefits of the system as portrayed by the end-user and limitations of the system technology.
- Chapter 12 includes the conclusion, lessons learned from the Case Study, some recommendations and options to be considered for any future development of the system. Finally, there is an emphasis on the benefit of the working partnership experienced during the course of this project.

2 Part 1. Background

The Police Complaints Authority (PCA) review on shootings by police in England and Wales from 1998 to 2001: Recommendation 21 calls for a review of methods used for recording the booking out of firearms. The majority of police forces currently operate a paper-based method of recording the firearms issue process using a form similar to that shown in Figure 1 below. Use of a paper form adequately maintains general information, but is reliant on officers maintaining high levels of good practice. However, forms can contain inaccurate data and historical information is difficult to retrieve from them.

The form is titled "ISSUE AND RETURN OF FIREARMS AND/OR AMMUNITION AND CS". It has a header with a crest and the title. Below the header are several sections:

- Command & Control Date:** A date field.
- Station:** A text field.
- Issuing Officer:** A text field.
- Date & Time of Issue/Return:** A text field.
- Reason For Issue (Brief Details):** A text area.
- RESPONSIBILITY FOR USE - SECTION 2 (CRIMINAL JUSTICE ACT 1967):** A section with a warning: "It is an offence under section 21(1) of the Firearms Act 1968 for a person to use a firearm or ammunition in the exercise of their duty or in the performance of their duty if it is not lawful for them to do so." It asks for the name of the person to whom the firearm is issued and the name of the person to whom it is returned.
- ISSUE/RETURN DETAILS:** A section with checkboxes for "ISSUED", "RETURNED", "LOST", "DAMAGED", "REPAIRED", "RECALIBRATED", "REWORKED", "REPAIRED & RECALIBRATED", "REWORKED & RECALIBRATED", "REPAIRED & REWORKED", "RECALIBRATED & REWORKED", "REPAIRED & RECALIBRATED & REWORKED".
- ISSUE/RETURN TABLE:** A table with 6 columns: TYPE, SERIAL NUMBER, MAKE, SHOW TIME, ISSUE/RETURN DATE, and ISSUE/RETURN OFFICER. It has multiple rows for recording items.
- COMMENTS:** A text area for additional notes.
- IF WEAPON IS USED, FORM 700 MUST BE COMPLETED ON COMPLETION, TOP COPY TO BE COMPLETED TO SUBSEQUENT FIREARMS SUPPORT.**

FIGURE 1. Typical weapons issue paper form

Advantages of introducing a computer-based system compared to a paper-based system:

- Links can be established to cross-reference information from a central database.
- An immediate audit is available.
- Produce an easy way to view weapons' issue status centrally.
- Volume of paperwork is reduced, especially for multiple issuing locations.
- Information can be linked to maintenance schedules or weapon condition.
- Is not dependant on legibility of handwritten information.

To aid data recording, some information from paper-based forms can be entered manually into commonly used databases or spreadsheets (e.g. Access or Excel). However, this is labour-intensive and introduces the potential for data input errors.

There are some commercially available systems that adopt other methods of recording weapons issue data using bar codes. Bar coding offers a method of unique identification and coding, however, bar codes are vulnerable to damage from the operational environment.

2.1 System requirements

It was essential that the system met the operational requirements set out by the Firearms Support Unit. The system would need to have end-of-line performance and efficiency benefits, and would be expected to not introduce difficulties or delays to the existing weapons issue process.

The user's requirements of the system are detailed in Appendix A, but can be summarised as:

- To meet the operational requirements.
- User-friendly system to be simple to operate and administrate
- To provide accurate weapons information data quickly (i.e. who has what, and where).
- To enforce weapons issue authorisation procedures.
- To provide weapons status and maintenance information.
- To permit and record transactions for both operational and training activities.
- To allow efficient and effective analysis of the data on weapons and ammunition.

The technical requirements of a system are:

- A method of uniquely identifying a firearms officer.
- A method of uniquely identifying a weapon.
- A rugged hand-held portable device to read the above identifiers and collect the data.
- A method of transferring data from the hand-held unit to the central database.
- A central database to receive, store, view and manipulate the information and to generate reports.
- A stand-alone management computer for restricted system administration.

2.2 Project objective

The objective of the project was to develop a stand-alone, computer-based weapons management system incorporating RFID tags. The system would then be used as a pilot to demonstrate how the technology can be applied to improve the recording of the weapons issue process and the day-to-day management of the armoury. The system would also aim to address the recommendations made by the PCA.

2.3 Methodology

2.3.1 User's operational requirements

The initial user's requirements were developed by an operational Firearms Support Unit who are the end-users responsible for the issue of firearms on a daily basis. The involvement of the end-user at this very early stage ensured that every step of the weapons issuing process was included within the specification for the system. For a computer-based system it is important that all the relevant data are captured at the various stages in the weapons issue process. The flowchart in Figure 2 below shows a typical weapons issue process broken down into its basic stages.

As the project progressed, this basic weapons issue process was enhanced and improved to give considerably more functionality to the user and provide additional management data. A flowchart to show these enhancements is provided in Appendix B.

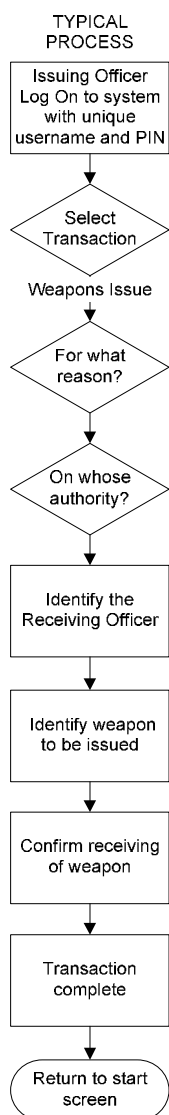


FIGURE 2. Basic stages of a weapon's issue

2.3.2 Technical specification

The user's requirement was examined closely by HOSDB and assessed for its technical viability. RFID tags have performance limitations and the appropriate technology selection and integration needed to be identified. From this assessment, HOSDB drew up a technical specification for the system.

At both the user's requirement and technical specification stages, it was important that the Force IT Department was consulted for its input regarding the specification of a computerised system. Though this project was specifically to develop a stand-alone system, some use was made of the existing network infrastructure.

Following successful system development it was envisaged that the Force IT Department would take full ownership of the system and be responsible for the day-to-day management of the system's integrity and security.

2.3.3 Tender process

The user's operational requirement and technical specification were incorporated within an Invitation to Tender (ITT) document and issued to possible suppliers. The tender submissions were evaluated on a competitive tender basis and contracts issued against the following criteria:

- Ability to deliver the work required.
- Technical expertise and relevant experience.
- Price.
- Ability to achieve the required timescales.

It was expected that any solution would:

- Be based on a Windows® operating system.
- Be based on an RFID data capture system.
- Have provision to fit new and replace lost/damaged tags and re-associate all relevant information.
- Ensure that tags in no way interfere with normal handling and operation.
- Have a master terminal based in the main armoury to provide full system administration/back-up/access/search/report facilities.
- Use rugged mobile terminals which capture and transfer data to/from the master terminal.
- Be an expandable system to allow additional types of assets to be added.

3 System fundamentals

3.1 Management computer

A desktop computer is used by the system administrator to configure the system, run searches and produce reports. The computer stores the database containing officer and weapon information. The administrator initially sets access rights for individual officers and the officers can then access the system by typing in their service number and a unique self-selected Personal Identification Number (PIN).

3.2 Overview of the issue process

The weapons issue process is managed entirely from a hand-held computer with an integrated RFID reader, as shown in Figure 3. The hand-held computer is used by the officer to log-on to the software by scanning their personal RFID card and entering their PIN. The software is menu-driven and users are led through the minimum number of steps necessary to complete the issue process. Data entry is performed by a combination of selections made using a stylus on the touch screen and reading the RFID tags with the hand-held computer. The system verifies with the database that the firearms officer currently holds the appropriate classification to be issued with a particular weapon type. The process also requires the receiving officer to self-certify that they are present during the transaction and their suitability (fitness) to carry firearms in relation to alcohol consumption, drugs use etc.



FIGURE 3. Hand-held computer

3.2.1 User options – issue, return and move weapons

To maintain the integrity of a computer-based management system, all of the weapons transactions carried out within the armoury are included. The system should have the functionality and capability to receive, record and store data to enable the management of the following transactions, and are shown in the schematic in Figure 4:

- Weapons issue:
- Operational use.
- Training.
- Retrospective issue.
- Weapons return.
- Movement of weapons.
- System administration (restricted access function only).

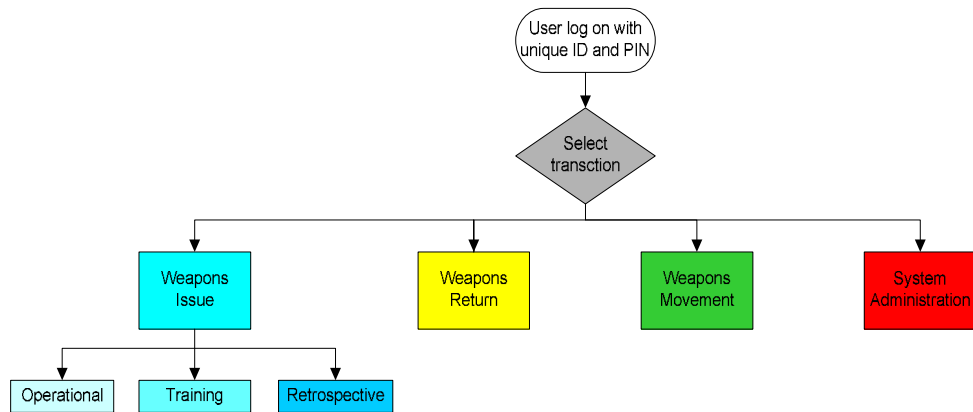


FIGURE 4. User options on hand-held computer

Figure 4 above shows the process and the options available to the user once they have successfully logged into the system. A brief description of each of the steps follows:

User Log-on to hand-held computer

Issuing officers log-on using their personal ID card together with their PIN. This screen is mandatory and is the start screen prior to access to any other options.

Weapons Issue – Operational

Initiates the process for an Issuing Officer to issue a Receiving Officer with a weapon(s) for operational use.

Weapons Issue – Training

Initiates the process for an officer with firearms training responsibilities to issue a weapon or multiple weapons specifically for training purposes.

Weapons Issue – Retrospective

Initiates the process for an officer to enter details retrospectively following a spontaneous issue of firearms.

Weapons Return

Initiates the process for an officer to return a weapon(s) back to a location following a weapons issue.

Weapons Movement

Initiates the process to log the movement of a weapon(s) from one location to another.

System Administration

This function has restricted access granted by administrators and is used to assign new RFID tags to the system.

4 The basic principles

The basic principle of the system is to determine a method to uniquely identify both firearms officers and weapons. For this application the system uses RFID tag technology. The RFID tag electronically stores a unique number which can be associated to an individual officer or weapon. The tags can be read electronically and can be produced in various forms. Figure 5 below shows examples of an identity card embedded with an RFID tag for use by officers and a thin laminated tag that can be adhered to a weapon.



FIGURE 5. RFID tag embedded in a personal identity card and an RFID tag in a laminate form

Using this technology, the principal objectives of the system are to:

- Issue each firearms officer with an RFID card.
- Place an RFID tag on each weapon.
- Electronically read and collect data and record transactions in a database.
- Identify weapon location.
- Generate information for audit and reports.

4.1 What is RFID and why use RFID in this application?

The fundamentals of RFID are dependent on a tag (or transponder) and a reader, as shown in Figure 6. The tag contains an electronic circuit that contains a unique identification code. The tags used in this application are referred to as 'passive' tags, which means they do not have a battery or power source on-board. The reader is connected to a power supply and emits radio waves so that when the tag comes within range of the reader, the tag is energised by the power of the reader and causes the tag to transmit its unique ID code, which is received by the reader.

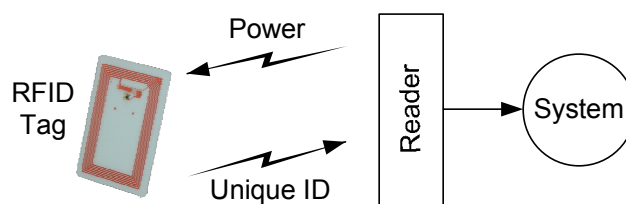


FIGURE 6. Principle of reading an RFID tag

The key features of RFID tags are:

- They transmit a unique ID.
- The unique tag information can be associated with database information.
- No power source is required – the tag is energised by the reader.
- They can be retrospectively fitted to the weapon.
- Short read range avoids spurious or accidental readings.
- No geographical information is gained from the process.

4.2 Identifying an authorised firearms officer (AFO)

It is usual for a police officer to hold a personal identity card of some kind. However, an AFO is required to hold additional identification to verify authority and status to carry firearms. Incorporating an RFID tag into an AFO's plastic identity card enables the card to be read electronically, making each cardholder uniquely identifiable by the system.

4.3 Identifying a weapon

Traditionally, a weapon's unique identifier is the serial number usually stamped on the main body of the weapon. When using a paper-based system to issue a weapon, recording the identity of each individual weapon relies on the physical reading and recording of the weapon serial number on a form. This method of manual administration is vulnerable to errors or inaccuracy of recording. Fitting an RFID tag to each weapon provides a method of electronically reading the unique identity of that weapon. After fitting a tag to each weapon, the tag number takes the place of the weapon's serial number as the unique identifier.

By coupling the ability to electronically read the officer RFID cards and weapons RFID tags with storing the relative weapons data in a computer database, weapons transactions can be captured and stored for weapons issue, monitoring and management reporting. Figure 7 represents a schematic diagram of this arrangement.

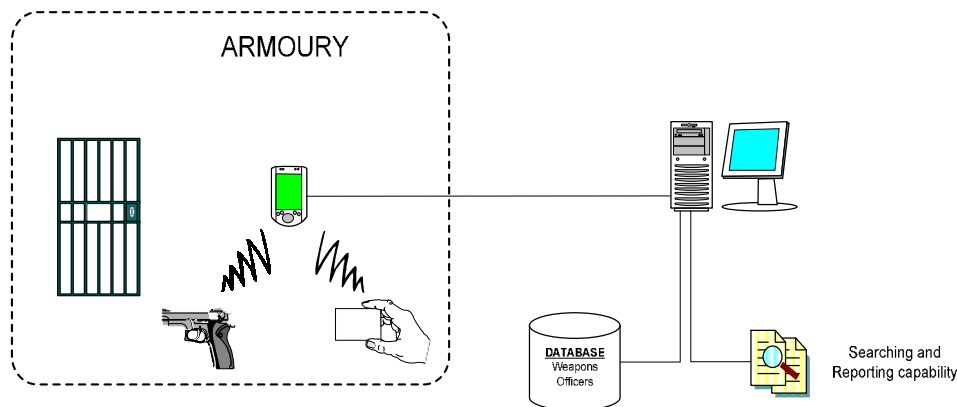


FIGURE 7. Basic system schematic diagram

4.4 Weapon RFID tags

For the purpose of this pilot demonstrator system, the tag type and form were determined in order to prove that the technology works for this application. For this reason, the tags were retrospectively fitted to all weapons. In the event of a damaged or faulty tag, it was necessary for the system administrator to have the ability to fit a replacement tag easily. Ideally, the tag would be embedded within the main body of the weapon where it is more protected.

The RFID tags used for weapons are produced in two physical forms and are in a format appropriate to the weapon type so as to meet the following operational criteria:

- They do not interfere with a weapon’s usual handling.
- They do not interfere with a weapon’s operation.
- They can be fitted in a place on the weapon where they are accessible to be read and replaced if necessary.
- They do not interfere with Electro-Muscular Disruption (EMD) devices (e.g. Taser®). This aspect has not been tested as part of this project.

Thin laminated self-adhesive tags were fitted to handguns and a tag was encapsulated within a plastic form and glued with a strong adhesive for long arms.

4.5 Handguns

There were a limited number of positions that a tag could be fitted to a handgun and still meet the operational criteria listed above in 4.4. The most suitable position was to stick the laminated tag (Figure 8) under the grip as shown in Figure 9 (circled). The tag location offered some protection and the advantage of a good position for presenting the reader to the tag as shown in Figure 10. This method may not be possible on all types of handguns.



FIGURE 9. Laminated tag fitted under the grip



FIGURE 8. Laminated tag



FIGURE 10. Reading the RFID tag fitted in a handgun

4.6 Long arms

There were a variety of long arms to be tagged, including rifles, shotguns and carbines. These are listed further on in the document in 8.2. An armorer identified locations where the tags could be fitted so that they would not interfere with the operational effectiveness of the weapon. Owing to the fact that the tags are encapsulated in rigid plastic (Figure 11), a flat face was required to give the most effective bonding surface. As can be seen in Figure 12 and 13.

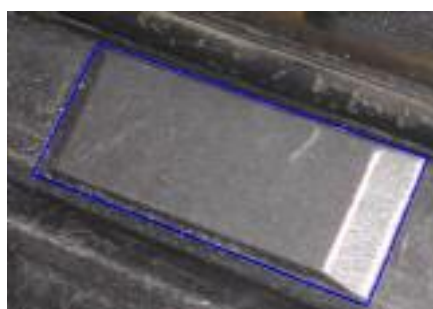


FIGURE 11. Tag encapsulated within rigid plastic and bonded to weapon body.



FIGURE 12. Tag fitted to G36



FIGURE 13. Tag fitted to MP5

The read range between the reader and the tag is just a few millimetres. This helps to make the reading of a weapon tag deliberate and avoids any erroneous readings.

5 User functions

5.1 Hand-held computer user functions

It is important that the system is designed to include all of the weapon transactions that it would be necessary to carry out within the armoury. In order to generate an accurate audit trail, it is a fundamental requirement that information generated from a weapons issue would also need to be reconciled by data being re-entered into the system at the point at which a weapon is returned; this is done by capturing or inserting data using the hand-held computer. Screen shots of the hand-held computer in Figure 14 show the user options.



FIGURE 14. Screen shots from a hand-held computer showing the user options

The start of each process involves a method of logging-on to the hand-held computer using an officer's RFID card in conjunction with entering their PIN using the touch screen. Successful log-on opens the next screen where the user can select from a list of options to: issue, return or move a weapon, initiate administrator function or log-out. If Issue Weapon(s) is selected then further options can be chosen for the type of weapons issue required: Operational, Training or Retrospective. More details on the individual processes are given in Chapter 10.

5.2 Management computer and reports

The management computer is used for system configuration and administration, and holds the database containing all of the information relating to the officers and weapons on the system. Defined management reports can be selected and hard copies printed. The computer runs on a Microsoft® Windows® operating system using the standard commands and controls.

As the system was under development, the end-user was encouraged to take part in the testing and evaluation of the system. Valuable feedback was provided and improvements were made to improve the functionality of the output of reports provided by the system. This partnership highlights the importance of user interaction to address the majority of issues that occur in the 'real-life' weapons issue process.

The computer-based system has the ability to carry out the following weapons management functions to address the requirements outlined in Appendix A and to include all the aspects of armoury management. A list of the system capabilities is given below, followed by an outline description of each function:

- Officer personal system log-on.
- Allocation of authorisation levels – management computer, hand-held computer, weapon types and access to the armoury.
- Issuing of weapons.
- Moving of weapons between locations.
- Returning weapons.
- Retrospective actions.
- Training (multiple) issues.
- Ammunition issue and stock control.
- Weapons maintenance.
- Fault reporting.
- System alerts.
- Access control
- Pre-defined or search capable reports can be generated and examples are explained later.

5.2.1 Logging in

The system administrator configures the system to allow officers the ability to log in to the management computer to gain access to a restricted number or all of the reporting functionality. To log in, officers are required to enter their service number and PIN at the log-on screen in Figure 15. During this set-up officers are associated to one of three access levels:

- Level 1 – change PIN only.
- Level 2 – run a selection of reports and change PIN.
- Level 3 – administrator level for full system control.

Levels 1 and 2 allow officers to access the system to change their own PIN. For obvious security reasons, officers are not permitted to select their Service Number or duplicate numbers, e.g.1122, to be their PIN.



FIGURE 15. Management computer log-on screen

Following successful log on to the system, a list of menu functions can be selected, though some functions are restricted to the System Administrator access. Below lists some of the functions outlined in 5.2 and brief descriptions.

- Weapons issue – identify the issuing officer, the weapon being issued and the receiving officer.
- Weapons movement – identify a weapon and its existing location, and select a new location to where the weapon is to be moved/has been moved. This location could be another armoury, grab bag or ARV.
- Returning of weapons – weapons that have been previously issued can be booked back into an armoury.
- Retrospective issues – where, for operational reasons, a full issue process cannot be carried out, retrospective issues can be done. This type of transaction includes all the necessary data that would be collected from a regulated issue. This ensures that the database remains updated with any transactions even after the event.
- Training issues – this process allows a firearms trainer to be issued with multiple weapons and ammunition in a single transaction. The process is recorded as ‘Training’ and avoids the issuing officer having to repeat the full issue process for each individual weapon.
- Ammunition – at the time of a weapon issue a standard quantity of operational rounds is also issued to suit the particular weapon. This quantity is then deducted from the stock ammunition. When a weapon is returned, the system prompts the officer to answer whether any operational rounds have been fired. Since rounds are very rarely fired, those originally issued are usually returned to the stock of the ammunition inventory.

- Weapons maintenance – the system will prompt the administrator when a weapon requires scheduled maintenance. This notification is initiated by a fault being reported following a weapons return or after a designated number of rounds being fired before required maintenance.
- Fault reporting – at the time of returning a weapon, the system allows the officer the opportunity to report any faults experienced with the weapon. The level of fault is categorised into Serviceable, Not Serviceable or Minor Damage. If Not Serviceable or Minor Damage are selected, an explanation is required which is logged in the database and flagged to the system administrator.
- System alerts – particular events may require immediate notification. The system can be configured to send appropriate pre-set SMS messages to a designated mobile telephone number for immediate attention.

5.3 Access control

The user's operational requirements in Appendix A also included the need to control access to the armoury. The weapons and armoury management system would also use the same database information to control the level of access to the armoury.

Authorised officers use their personal firearms RFID card to access the armoury in conjunction with their personal PIN to verify their identity. All attempts to access the armoury using the cards, whether successful or not, are logged and stored by the system so each attempt can be monitored by the system administrator.

It is possible for an audit trail of weapons issue data to be collected without introducing access control. For this reason, it could be considered as a beneficial add-on to the system, giving increased control and improved management to the armoury.

6 Technical specification - system enhancements

As the system was being developed, there were opportunities to introduce some technical enhancements to the system delivering an even more seamless audit trail for the issue of weapons, and for armoury management. By using existing technology the system has the capability to transmit weapons issue data from remote locations back to the main database, delivering near real-time data recording. These enhancements could be deemed as not essential to a weapons and armoury management system, however, they would certainly be encouraged as introducing good practice.

The capability of the system was enhanced by the introduction of:

- Wireless data transfer.
- Wireless system updates.
- SMS (short message service) text alerts.

6.1 Wireless data transfer

To enhance the system from this static capability, the possibility of capturing the issue process out in the field was proposed. This would improve the capability of the system to allow the recording of the full issuing process from an Armed Response Vehicle (ARV), mobile armoury or remote location, and have the ability to immediately transmit those data to the management computer at Headquarters and update the database, as shown in the schematic in Figure 16. Data are transmitted via the mobile telephone network, Global System for Mobile (GSM), to update the database and give a near real-time reporting capability

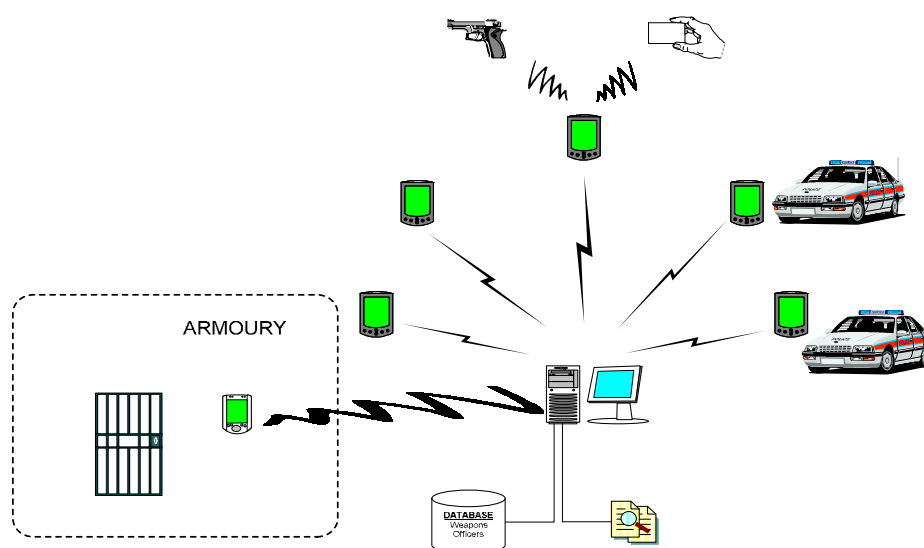


FIGURE 16. Generic wireless schematic showing data being transmitted from remote locations

6.2 Wireless system updates

This functionality excludes the possibility of the hand-held computers falling out of synchronisation with the main database (i.e. a discrepancy between the weapons or officer data on the database and the data on the hand-held computers). The system has been designed to update the hand-held computers after the completion of each weapons transaction. In addition, the hand-held computers contact (dial-in) the management computer at pre-set periods of the day to receive any updated information. Ideally these times should be selected to be at quiet periods of the day, e.g. between shift changes, when the data transmissions are less likely to be interrupted. This feature ensures that the hand-held computers store the most up-to-date information and the weapons computer database remains updated to provide a seamless audit trail.

6.3 SMS text alerts

The system was enhanced to enable SMS text messages to be sent automatically by the system to a dedicated mobile telephone number. The system can be configured to initiate such alerts at a number of critical situations where immediate notification would be advantageous. Details and examples of system alerts and associated text messages are described in Chapter 11.

7 Part 2. Case study

7.1 Introduction

The case study includes details of an installation of the demonstrator computer-based weapons and armoury management system in a Firearm Support Unit of a UK police force. Part 1 provided the background for the development of the system from the initial concept, and the technology used. Part 2 of the report explains some features specific to a particular armoury location and the on-going development of the system which were particular to the requirements of this police force.

The experience gained from the development of the system is outlined, and this part will conclude in Chapter 12 with a summary of lessons learned, recommendations and consideration of further possible developments.

7.2 User and operational requirements

Appendix A outlines the initial operational requirements set out by the user and how the system was designed to meet each of the requirements in turn. In addition to meeting all of these requirements, it is important that the new system takes into account the existing working procedures of the firearms officers. The adoption of any new systems or procedures, particularly involving the transition from a paper-based system to a computerised one, should not impede or take longer than the existing working practices.

Throughout the Case Study and system development the Firearms Support Unit maintained the ability to carry out their normal duties and access their weapons quickly in order to respond to firearms incidents.

7.3 Physical location

The Case Study location comprised two armouries in two separate buildings separated by a roadway. Computers housed at both armouries are connected by a dedicated fibre optic link. Figure 17 shows a schematic of the system layout.

Armoury 1 – this is the main armoury that holds the majority of weapons and has a working area for weapons maintenance. There is one main entrance door into the armoury. Inside, the armoury is split into two areas separated by a locked gate. Both the main entrance door and inner gate are accessed using an access control system, though a higher level of access needs to be granted to enable access through both the main door and the inner gate. It was identified that this location would house the Master computer.

Armoury 2 – this secondary armoury is a small armoury used to house mainly handguns for personal daily issue of sidearms to ARV officers. Entry to Armoury 2 is by an access control system. The administration computer is housed in a back office in close proximity.

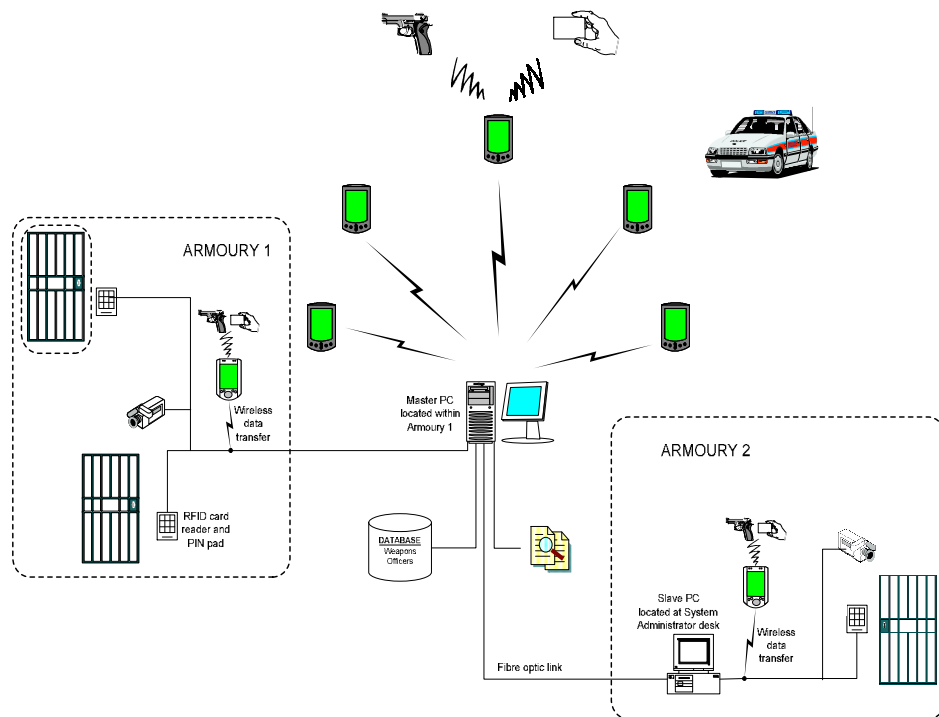


FIGURE 17. Schematic layout of Case Study installation

8 System description

8.1 Firearms officers' cards

For the Case Study police force, all firearms officers are issued with a personalised firearms RFID card displaying their name, service number and photograph. The RFID card stores a unique ID that can be read electronically and can be associated to the officer and their unique individual PIN. This enables the card to be used as a visible ID card, an access control card to the armouries and to log-on to the hand-held computers to verify the cardholder's identity.

Though this card identifies a firearms officer as authorised to be issued with a firearm, the system administrator has the ability to disable a card from the system, making the officer 'unauthorised' and preventing the card from being used to access the armoury.

8.2 Weapons tagged

A selection of commonly issued weapons was identified (Figure 18). The weapons were examined by a firearms supervisor to identify a suitable place to mount a tag where it would not obstruct handling or operation.

RFID tags were fitted to the following weapons:

- H & K MP5.
- H & K G36.
- SIG 226.
- Remington rifle.
- L104A1 launcher.
- SIG 3000.
- Remington shotgun.
- Benelli shotguns.



FIGURE 18. A selection of weapons identified to have RFID tags fitted

Note. In this project RFID tags were not fitted to Taser®. Further testing would be required and advice should be sought from the suppliers and manufacturers.

8.3 Locations

For the purpose of the database, locations are defined in order to identify the current position of a weapon. For this Case Study, weapons would be associated with the following locations, defined as:

Home Office Scientific Development Branch

- Main armoury.
- Secondary armoury.
- ARVs (ARV1, ARV2...)
- Tactical Support Vehicle (TSV) as a mobile armoury (Figures 19 and 20).
- Grab bags/case (Grab Bag 1, Grab Bag 2...) (Figure 21).



FIGURE 19. Tactical Support Vehicle (TSV)



FIGURE 20. Hand-held computer in vehicle mounting cradle fitted in the TSV



FIGURE 21. RFID tag fitted to a grab case

8.4 System architecture

The computer-based system was developed particularly for the application of weapons and armoury management. The following are the key aspects of the Case Study system:

- Technology.
- Hardware.
- Data transfer.
- Software.

8.4.1 Technology

The system was devised from a variety of existing technologies integrated with readily available hardware. The system technologies included RFID tags and readers, webcams, a Windows[®]-based computer, electro-mechanical locks, and a hand-held computer with the capability to read RFID tags and transmit data wirelessly.

8.4.2 Hardware

- Hand-held computers.
- Desktop computer.

8.4.3 Hand-held computer

The requirements of the hand-held computer listed in the initial technical requirements outlined in Chapter 3 were:

- A rugged hand-held portable device to read identifiers (weapons, officers) and collect the data.
- A method of transferring data from the hand-held unit to the central database.

As the system developed, these requirements were expanded to specify:

- A fully integrated rugged hand-held unit with the ability to read RFID tags and to be easily portable for operation within an armoury, out in the field or from an ARV, and able to transmit data wirelessly back to a central database.

Identifying a suitable product that met all of these requirements proved much more difficult than first anticipated. There is a vast array of pocket PCs, PDAs and rugged mobile data recorders available on the market, but only a limited number that would meet all the requirements demanded by this application. A fully integrated unit with built-in wireless communication and the ability to read RFID tags fitted to weapons is such a specialised product that identifying one proved a considerable challenge.

Seven hand-held units were procured in total, of the type shown in Figure 22. Visually and operationally the units are almost identical, but are of two distinct types. This was to incorporate the two different methods of transferring data from the hand-held computers to the database, as explained

in Table 1 below. In this Case Study the physical location and construction of the armouries would prevent reliable GSM network coverage from being obtained (similar to problems with radios or mobile phones). To overcome this difficulty, Wi-Fi units were used in these locations.



FIGURE 22. Hand-held computer with RFID reader fitted and in desktop cradle

Type	Quantity	Wireless Data Transfer by:	Description of use
1	2	Wi-Fi	Used within both armouries to send data locally from the hand-held unit to the database.
2	5	GSM	Deployed in ARVs or at remote locations to send weapons issue data back to database at HQ.

TABLE 1. Different types of hand-held computer and their uses

8.4.4 Transmitting data wirelessly – externally and internally

The benefit of wireless data transmission is that weapons transaction data can be sent immediately from any location, updating the database in near real-time.

(a) Externally

Data are sent and received between the hand-held computers and the system computer at HQ via GSM. The hand-held computers with GSM capability are used in the ARVs or at off-site locations to send and receive weapon transaction data. Each GSM unit requires a SIM card, identical to that found in a mobile phone and also involving line rental and call charge costs, to dial-in to the system to send and receive data. The management computer sends and receives data from the hand-held computers via a dedicated ISDN telephone line installed at HQ. In the eventuality of a GSM unit failing to establish contact with the system, the hand-held unit will attempt to re-dial three times.

(b) Internally

Obtaining a GSM signal within the armouries proved difficult and unreliable owing to their physical location and construction. Therefore, an alternative method of wireless data transmission was employed by selecting a hand-held computer with Wi-Fi capability. The Wi-Fi units transmit data locally from within the armoury between the hand-held units and a wireless receiver connected to the management computer. This set-up was replicated in both armouries.

A less acceptable alternative to transmitting data wirelessly would be to transfer the data captured by the hand-held units by physically docking the units in a cradle hard-wire connected to the database computer. Docking would initiate the downloading of the data. However, until docking, the information would remain stored within the hand-held computer and the database would not receive up-to-date information, potentially leaving loopholes in the audit trail.

8.4.5 Desktop computer

Two identical desktop computers were supplied to manage the system between the two armoury locations, connected by a dedicated fibre optic link. The computers are used to set up and manage the system, configure and modify settings, and produce and view weapons management reports.

Additionally, connected to one of the computers is a dedicated back-up system (DAT drive) to enable full scheduled system back-up, and a GSM modem to send system SMS alerts, which are described in more detail in Chapter 11.

8.4.6 Management reports

Data captured on the hand-held computers are transferred to the stand-alone management computer, updating the database. The database information can be manipulated to enable searches, queries and a variety of pre-defined reports to be selected. The majority of report types were defined in the original user requirements. Hard copies of each report can also be printed.

Below are some examples of the pre-defined reports and a description of their functionality, followed by some example screen shots of the report page:

Weapons Currently Issued – lists weapons currently issued for operational use (shown in Figure 23).

Authorisation Levels – lists officers and their authorisation level.

Total Inventory – lists all the tagged weapons logged into the system held by the armoury (shown in Figure 24).

Weapons due for Maintenance – lists weapons highlighted for maintenance and last maintenance date.

Inventory by Location – search can be made to list weapons housed at a particular location.

Unauthorised Officers – provides a list of officers who have had their classification temporarily suspended by the system administrator for whatever reason, e.g. a failed fitness test or training shoot.

Unauthorised Issuing – provides a report of weapons issued where authority was over-ridden (explained in Chapter 9).

Weapons Ammo Usage – provides a report on rounds fired for each weapon.

Defective Weapons – lists weapons reported as defective.

Officer History – lists the transactions made by a particular officer.

Weapons History – lists the details the transaction and status history of an individual weapon.

Access Log – lists a history of access attempts to the armoury.

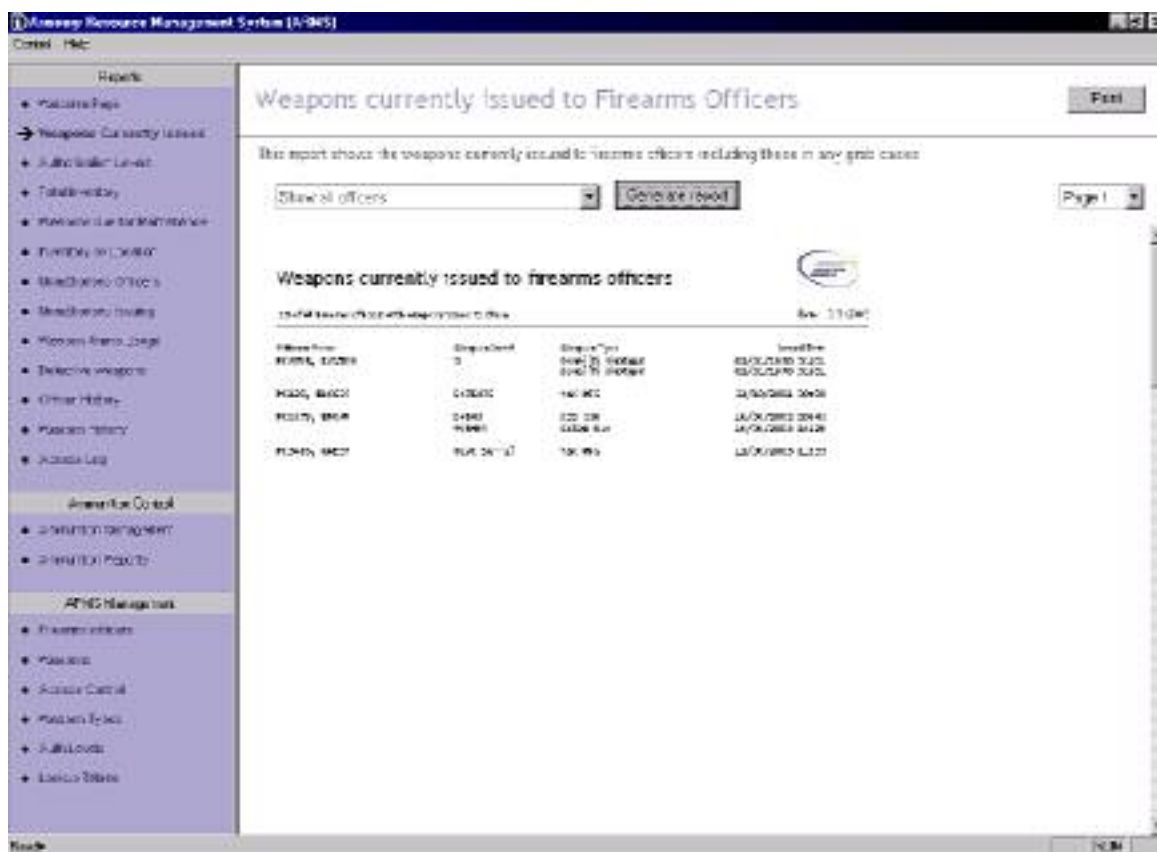


FIGURE 23. Example of a report showing weapons currently issued to all AFOs. This list can be refined to show weapons currently issued to individual AFOs

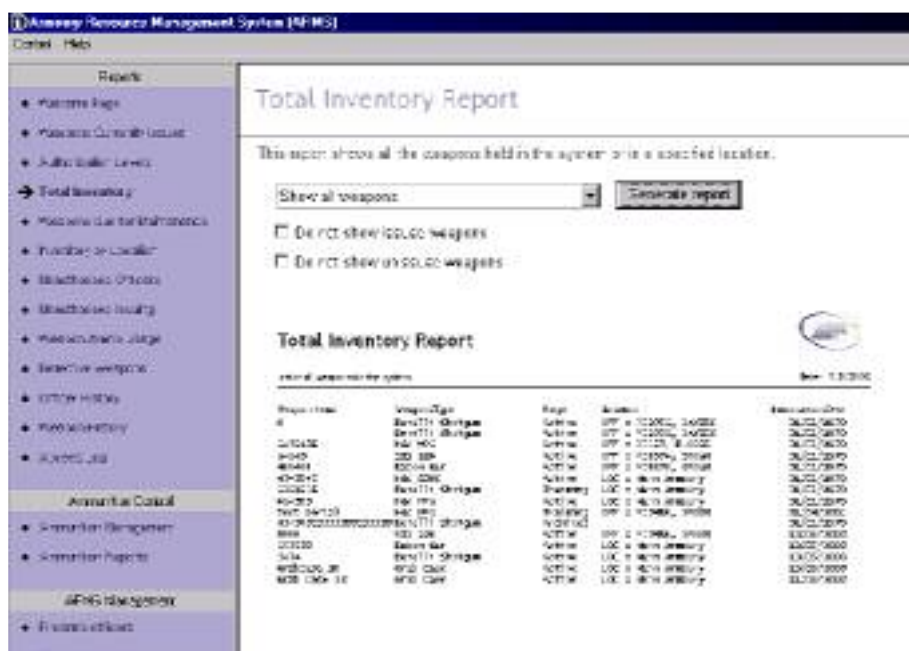


FIGURE 24. Example of a Total Inventory Report

8.4.7 Authorisation levels – weapons issuing

The user requirements highlighted the need to verify that an officer has the correct authorisation (classification) to be issued with a particular category of weapon. Officer authorisation level is set to distinguish between officers with basic training level requirements, instructors and administrators and this is configured by the system administrator on the management computer.

8.4.8 Unauthorised issuing

In the event that an unauthorised issue is attempted, e.g. an officer only trained in the use of a shotgun and baton gun attempts to self-issue a sniper rifle, the system verifies the officer’s authorisation level with corresponding information stored in the database and will notify the officer of the pending ‘Unauthorised Issue’. In recognition that this type of transaction would be necessary for operational or training situations, the transaction is still permitted, but initiates a record of the event. Firstly, the hand-held computer prompts the user with a text box, informing them that they do not have the authority to be issued with that category of weapon (Figure 25). Before proceeding, the user must verify that they are willing to override the authority in order to continue with the issue process. The next screen prompts the officer to insert a reference for the officer authorising the override (Figure 26). This type of transaction is logged on the management computer and a report entitled ‘Unauthorised Issuing’ can be generated (Figure 27).



FIGURE 25. Officer not authorised



FIGURE 26. Reference for override notification



FIGURE 27. Example of Unauthorised Issuing report

8.5 Ammunition

The system holds inventory data for ammunition stock. Rounds of ammunition are booked out with a weapon issue and booked back in during a weapons return (as shown in Figure 28).

The number of rounds fired is linked to weapons maintenance records and the armourer is notified when a weapon is due for routine maintenance.

For reporting purposes, the system differentiates between rounds fired during training and those for operational issues.

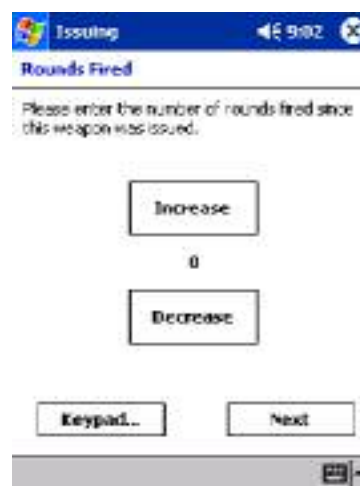


FIGURE 28. Rounds Fired screen

Reports on ammunition usage can be generated and hard copies printed (as shown in Figure 29).

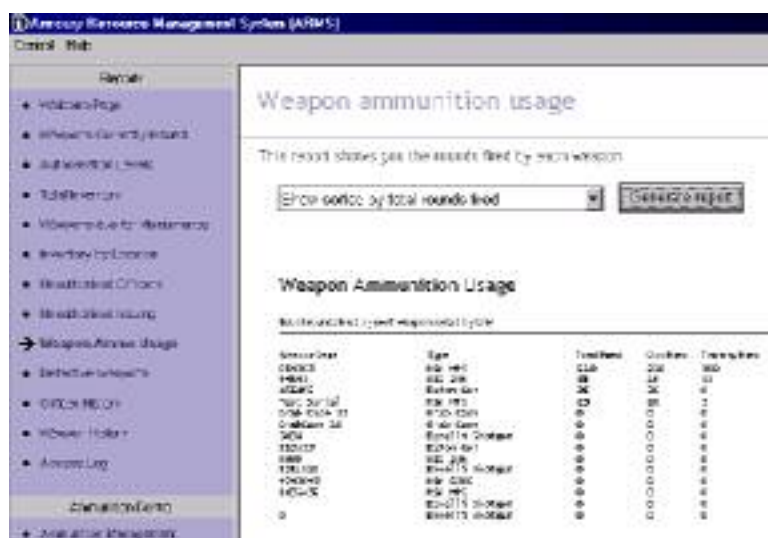


FIGURE 29. Example of Weapon Ammunition Usage report

Administrator access allows full management and production of ammunition stock control reports, as shown in Figure 30. Ammunition types can be added, modified or deleted and the inventory levels can be fully controlled by amending any incoming or outgoing quantities of ammunition.

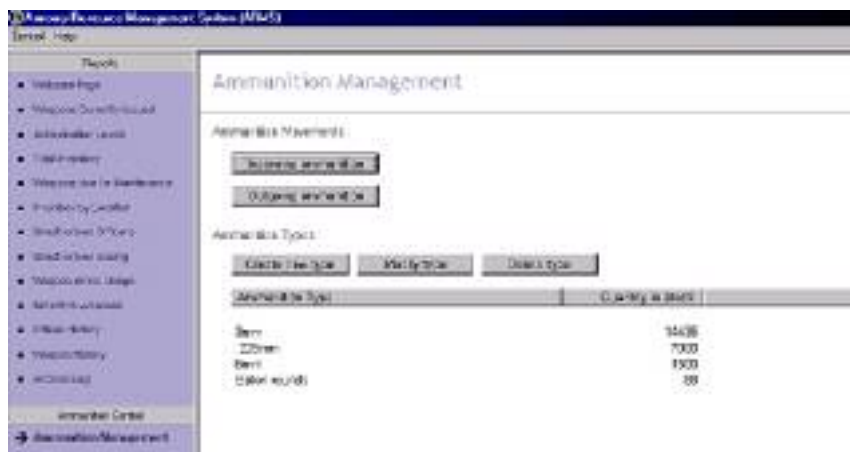


FIGURE 30. Example of Ammunition Management report

9 Description of the processes - weapons issue, return, movement and administration

The electronic capture of the data from the RFID tags makes the data collection process easier than recording on a paper system and the management of the issue of firearms more accurate and reliable. This chapter explains each of the processes in turn. There is a brief explanation of some key stages in the process accompanied by some example screen shots from the hand-held computer.

The hand-held computer provides the user with the following options:

- Weapons Issue – for Operational use, Training use or a Retrospective issue
- Weapons Return
- Weapons Movement
- System Administration.

The hand-held computer guides the user through each of the processes, following a step-by-step procedure. The Issue, Return and Movement procedures can be followed in more detail in the flowcharts of each process in Appendices B, C, D, E and F.

9.1 Weapons issue – operational

The flowchart in Appendix B shows how the fundamental steps in the issue process in Figure 2 were expanded to give more functionality. These additional stages provided opportunities to capture further data, leading to tighter, more detailed audit control. The flowchart in Appendix B can be followed through the following stages of a weapons issue for Operational use. For this scenario the user had the requirement that an *Issuing Officer* would manage the process of issuing a weapon to a *Receiving Officer*.

Identification – both issuing and receiving officers are able to uniquely identify themselves to the hand-held computer by scanning their personal RFID firearms officer identity card. Personal identification can be verified by the user entering their personal identification number (PIN) on the touch screen as shown in Figure 31 to confirm they are actually in attendance at the time of the transaction.



FIGURE 31. Log-in screen

Authorisation – supplying a list of approved named options (Figure 32) that have the authority to endorse the issuing of firearms helps to enforce the necessary protocols.



FIGURE 32. Selection of authorities

Accuracy – scanning weapon RFID tags maintains the accuracy of weapon identification. Scanning the tag will display all the information specific to each weapon as shown in Figure 33. A paper system that requires time-consuming manual insertion of a weapon serial number comprising several digits is open to possible input error.



FIGURE 33. Specific weapon data

Procedures – in accepting the issue of a firearm, a firearms officer is expected to confirm acceptance of the following self-declarations:

- Section 3 Warning
- Fitness for Duty.

Figure 34 below shows the details of these declarations that are included in the stages of the weapons issue procedure and the receiving firearms officer is required to acknowledge that they have read the declarations by scrolling down the text and ticking a check box. In order to confirm that the receiving officer is actually present to acknowledge these declarations, the next stage in the issue procedure asks for the receiving officer’s PIN. (Entering a unique PIN is considered as an acceptable substitute for a signature.)

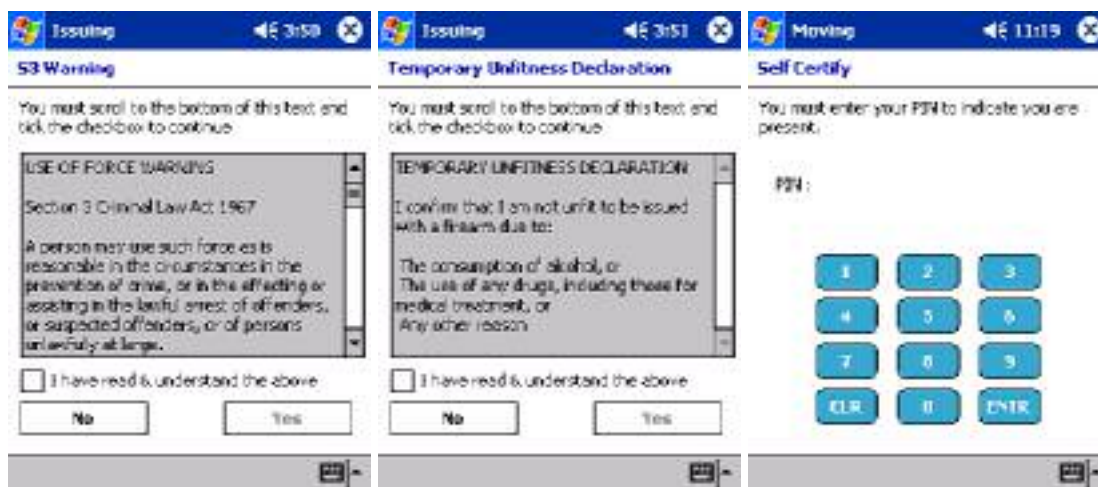


FIGURE 34. Self certification screens

9.2 Weapons issue – training

When issuing weapons for a training shoot, an instructor is likely to issue several weapons per session. The system process for issuing weapons for training has been developed with this in mind and to meet the user’s operational requirements. Issuing weapons for training purposes is a simplified version of the individual weapons issue process. Details of the full process can be followed using the flowchart in Appendix C.

Following the mandatory log-on screen and selecting Weapons Issue function, only officers who have been assigned **Instructor** level of authorisation can proceed to access the issue for training use function by scanning their RFID card as shown in Figure 35.



FIGURE 35. Identify instructor screen

As instructors are likely to issue a number of weapons, perhaps of different types, this process allows more than one weapon at a time to be scanned and generates a list of the weapons selected for training as shown in Figure 36.



FIGURE 36. List of weapons scanned to be issued for training

The instructor must then enter the number of rounds of ammunition required for training for each weapon type as shown in Figure 37. If all of the weapons in the list use the same type of ammunition, just one figure is entered for total rounds required. However, if a variety of weapons have been selected, this screen toggles through the ammunition types corresponding to each weapon on the list and the rounds are entered in turn.



FIGURE 37. Rounds issued screen

The two closing stages request the instructor to confirm that they are issuing the weapons for training purposes and include a reminder to carry out a weapons function check.

9.3 Weapons issue - retrospective

In the event of an officer having to spontaneously self-arm with a weapon in order to deal with an incident, there is no time to carry out the issue process using the hand-held computer. The system allows the officer to retrospectively enter the details of the weapons issue on the hand-held computer. Once completed, the details of the issue can be transmitted back to HQ, updating the database and enabling near real-time reporting and monitoring. Details of the full process can be followed using the flowchart in Appendix D.

Following the mandatory logging in screen and transaction selection, post-event, the officer can enter the original date and time of the spontaneous issue as shown in the Figure 38.



FIGURE 38. Screen to enter date and time of a retrospective issue

The system offers a selection of pre-defined reasons for the retrospective issue as shown in Figure 39. In the event of a system fault, the hand-held computer will accept manually inserted data and store them within its memory. When the fault is rectified, the data stored in the hand-held computer can be transmitted back to HQ.



FIGURE 39. Select a reason for retrospective issue

Figure 40 shows the next screen prompting the user to confirm the weapon has been returned. It is important that the weapon is returned through the system in order to maintain the accuracy of the audit trail. SMS alerts are issued as a consequence of a weapon being out on issue for over 14 hours. This is described in SMS alerts in Chapter 11.



FIGURE 40. Confirm weapon has been returned

9.4 Weapons return

For the integrity of the system and to avoid generating any disparity in the audit trail, it is important that the weapons issued through the system are also returned through the system. Weapons are returned to pre-defined locations. During the weapon return process, the officer has the opportunity to enter a reference (URN) that may relate to the reason for the original issue, number of rounds that may have been fired and the condition of the weapon on return. Details of the full process can be followed using the flowchart in Appendix E.

Following the mandatory logging-in screen and transaction selection, the location to where the weapon is being returned can be selected from a pull-down menu of options. The locations are pre-defined by the administrator and could be the main armoury, grab bag, ARV or remote armoury. Alternatively, a location can be manually inserted as free text using the touch screen keyboard as shown in Figure 41.



FIGURE 41. Screen to select where weapons have been returned to

As a reference to the original weapons issue, an incident reference number, URN or free text date-related entry can be made as shown in Figure 42. Alternatively, **Training** can be selected and is automatically entered into the text box.



FIGURE 42. Screen to enter a reference relating to the firearms issue

To maintain the ammunitions inventory, the stock of each type of ammunition is adjusted when a weapon is returned. The number of rounds fired can be entered using the Increase and Decrease buttons or by manually entering the quantity using the touch keypad as shown in Figure 43.

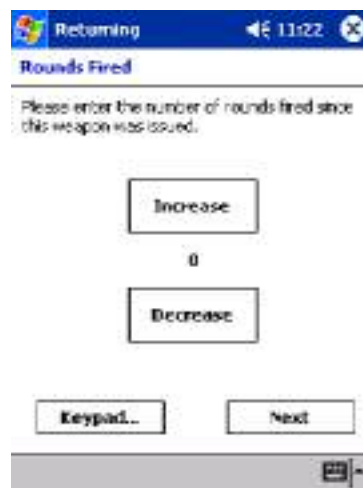


FIGURE 43. Screen to enter number of rounds fired

When a weapon is returned, the officer is requested to report the condition of the weapon. One of the following three options must be selected as shown in Figure 44:

- Serviceable – no faults.
- Not Serviceable – major fault – any future issue will be denied.
- Minor Damage – armourer notified – future issue allowed.



FIGURE 44. Status of weapon being returned

Selection of Not Serviceable or Minor Damage prompts the officer to select Enter Fault Description as shown in Figure 45. This opens the next screen and the officer must enter a description of the fault by using the touch keyboard. The system alerts the administrator to any weapons reported as defective.



FIGURE 45. Enter description of fault

9.5 Weapons movement

On the occasions when weapons are required to be moved from one location to another, the weapons movement transaction is selected. To maintain the integrity and accuracy of the data held in the database, all movements of weapons should be logged through the system. This provides accurate management data to establish the location of weapons at any given time. Details of the full process can be followed using the flowchart in Appendix F.

Following the mandatory logging-in screen and transaction selection, the officer responsible for moving the weapons scans their RFID card to prove identification. The location to where the weapons are being moved is selected from the pull-down menu of locations pre-defined by the administrator. Alternatively, a location can be manually inserted as free text using the touch screen keyboard. If a number of weapons are being moved, the next screen will generate a list of all the weapons scanned to be moved. This transaction is a simplified version of the weapons return process.

9.6 Administration

Only officers with administration authorisation level have access to this function. Selecting **Administration** on the hand-held computer opens the next screen displaying the option to issue a new tag to a weapon or issue a new card to an officer as shown in Figure 46.

- **Issue new tag to weapon** – goes through the process of assigning a tag to the weapon serial number and would be used:
 - When a new weapon is tagged and entered on to the system.
 - When there is replacement of a defective tag on a weapon.
- **Issue new card to officer** – goes through the process of assigning an officer's RFID card to their service number and would be used:
 - To issue a new RFID card to an officer and enter the details on to the system.
 - When a replacement for a defective RFID officer card is required.



FIGURE 46 Administrator functions available to issue new tag or cards.

10 System features

10.1 Access control

For this case study, there was an opportunity to integrate an access control capability linking both armoury locations. Previously, a high level of good practice was required to manage access to the keys to the two armoury locations. Introducing access control capability to the system gave an opportunity to replace the existing arrangements and to develop a 'keyless' system (although the locks may be electro-mechanically operated, each lock has mechanical key override).

To manage the weapons issue process it was not essential to integrate access control capability, however, it was successfully implemented in the Case Study. The additional functionality provided valuable management information for the audit trail and to the administrator in determining who attempted access, where and when.

Firearms officers must use their RFID card to gain access to both armoury locations. The administrator must assign an appropriate level of access dependent on an officer's authorisation. For example, a higher level of authorisation is required to gain access through the inner gate within the main armoury.

Features of the access control system include:

- An officer is required to present their RFID card to the wall-mounted reader and must verify their identity by entering their unique PIN on the keypad, as can be seen in Figure 47.
- A webcam (Figure 48) takes a digital photograph that is date and time stamped:
 - To address the possibility of attempted misuse and lending of personal cards
 - To verify the holder visually
 - The image is stored and can be accessed in the event of an armoury access enquiry.
- Any failed attempts at PIN entry are displayed as RED on the access report screen to highlight it to the system administrator for possible investigation. The image of this event can be easily recalled.
- Only three failed attempts at PIN entry are permitted, after which an officer will be locked out of the system. The system administrator must reset access permissions.
- SMS alerts of attempts to gain entry by officers who have been made unauthorised by the administrator and where their classification has been suspended.



FIGURE 47. Presenting RFID card to door access control reader with keypad



FIGURE 48. Webcam positioned above armoury entry doors

10.2 Typical system notifications

As part of the management and monitoring capability, the system produces both internal and external notification messages to a system administrator or designated receiver.

10.2.1 Internal

- Welcome screen – following log-on, the system administrator is presented with a tasks screen. This provides a summary of any events that have been flagged for attention, e.g. failed attempts to access the armoury or overdue weapons.
- Authorisation override for weapon type issue – if an officer attempts to carry out a self-arm issue of a weapon type (e.g. rifle) when they do not have the designated authority or classification to be issued with that particular category of firearm, the system will notify the officer of this pending action. The system will question the officer as to whether they have a requirement to override this request for authority. Acceptance of this overriding action is logged within the database and a query report can be run to list details of the action.

- Weapon faults – following a weapon with a major fault being returned as Not Serviceable, any future attempts to issue the weapon will be denied until the fault is rectified and the system administrator has re-enabled the weapon fit for issue. Following a weapon being returned with Minor Damage, future issues are permitted and the system administrator is notified that the weapon may require attention. When a returning officer selects either of these levels of fault, they must enter a plain text description of the fault. This information then appears to the administrator to enable them to take the appropriate action.

10.2.2 External SMS alerts

The system can be configured to generate and send alarm notification via a Short Message Service (SMS) text message to a designated mobile telephone number. There are specific requirements for external notifications. The alerts would be of a serious nature and would require an immediate response action. Selection of external alerts should be given due consideration so as not to generate an excessive amount of messages or create the possibility of unnecessary false alarms that would cause a nuisance and the likelihood of this functionality being disabled. Table 2 below shows some examples of the types of alarm that will generate an SMS alert.

Alert	Example Text Message	Description
Unauthorised officer attempts entry.	"Officer:1234, SMITH tried to access an armoury, but they are unauthorised"	If an officer has been made 'unauthorised' by the system administrator and then attempts to enter the armoury, this message will be sent.
More than three attempts at PIN entry.	"Officer:1234, SMITH has had their access to the system disabled due to 3 failed attempts to login"	If an officer attempts to gain entry and has three failed attempts at PIN entry then the third failed attempt will generate the alert message.
Weapon issue longer than 14 hours (shift).	"Weapon ABCD12345 has been with officer 1234, SMITH for over 14 hours"	If the issue period for a weapon is in excess of 14 hours without going through the return process, an alert message will be generated.
Card not known.	"Someone with card :000123 has tried to gain access to an armoury"	If an attempt is made to enter the armoury with a card not known to the system, an alert message is generated.

TABLE 2. Examples of SMS alerts generated by the system

10.3 System security

The system was not designed to include high security measures to physically prevent an authorised firearms officer from performing their duty and accessing firearms on a day-to-day basis. Where practicable, some security features have been built-in to the system.

The system incorporates a variety of levels of security to identify and verify users at various stages:

- Personal RFID enabled identity card with holder's name, service number and photograph.
- Access entry requires RFID card plus PIN entry verification. Additionally, a digital photograph is taken at the point of entry.
- ID card plus PIN entry verification access to hand-held computers.
- Service number plus PIN log-on for computer access.
- PIN is self-selected and unique to individual officers. System prevents the officer using their service number as their PIN and does not allow any duplicate numbers, e.g. 1122, 6677.
- Administrators can set a range of authorisation levels for weapons issue category, access to the management computer and reports, and access to functions on the hand-held computer.

The benefits of the system are as a management tool to record the process for the audit trail. The system has not been designed as a high security measure and will not prevent the transactions from being attempted or completed.

This demonstrator system is constructed as a stand-alone network between two computers; it is not connected to the police IT network in any way. Any future developments should be discussed in depth with individual IT network departments for security assessment, before any consideration is given to connection with the police force IT infrastructure.

10.4 System training

It is important that any new systems capture all the relevant information and do not complicate any existing procedures. Intuitive, work-based training packages, including hands-on exercises, familiarise users to the system and the associated hardware. Users should be able to follow a simple, menu-driven step-by-step procedure prompting the user through each process. Such a user-friendly system has the advantage of gaining user acceptance and an understanding of the process required to capture the data, inevitably reducing the likelihood of both user and data input errors. Ultimately, the data held by the system and the reports generated are only as accurate as the data captured or entered by the users and administrators.

Suggested forms of instruction and training are:

- A PowerPoint® presentation giving an overview of the system, its capabilities and limitations using screen shots.
- Hard copy notes.
- Hands-on practical exercises.

At the training stage it is important that the myths and misconceptions regarding RFID tagging in this application are dispelled. The system technology does not have the capability to actively track movement or locate people or firearms geographically. However, as part of the user's requirements, the location of a firearm can be determined by running reports from the management computer. The location of a weapon is determined from the pre-defined armoury areas configured in the system by the administrator, e.g. Armoury 1, Armoury 2 or ARV 1. This information is recorded within the database when an officer has completed a firearms return or movement process.

10.5 Rough order of cost

A rough order of cost for a stand-alone system based on the requirements delivered in the case study is estimated at £50k and comprises two armoury locations and the following:

- Armoury management software.
- 1 master computer.
- 1 slave computer.
- 7 hand-held computers.
- 250 weapon tags.
- 50 RFID firearms officer cards.

Additional costs would need to be allowed for:

- Installation – this should be addressed as a site-specific requirement.
- Fitting of tags.
- Supply and installation of an access control system.
- Landline or mobile network charges and other running costs.
- Any further software developments.
- Support and maintenance of the system.

10.6 Benefits of the system

- Central administration, monitoring and reporting.
- A clear, unequivocal audit trail is generated.
- Once familiar with the system, it has been proved that the process of issuing and returning weapons takes less time than operating a paper-based system.
- Supervisory benefits, improving the safety and security aspects of armoury management.
- Electronic reading of unique identifier eliminates manual errors reading serial numbers.
- The system can be configured as a prompt for a confirmation action to be undertaken by a firearms officer:
 - Weapon check.
 - S3 Warning.
 - Temporary Unfitness Declaration.
- The system highlights weapon faults to the system administrator and prevents the ability to re-issue until a repair is carried out and the administrator reinstates the weapon on the system.
- Maintenance schedules can be set. The system will notify the administrator when a weapon is due for maintenance.
- Ammunition inventory. Though it would not be practical or cost-effective to place an RFID tag in each round, the system offers the ability to manage levels of ammunition stock held and ordering levels more efficiently.
- Intuitive use and training, using graphics where possible as shown in Figure 49.



FIGURE 49. Example of using a graphic to help in verifying data input by the user

10.7 Limitations

Issues for consideration encountered during the case study were:

- Awareness of metal on weapons. Tag reading performance is likely to be affected when the RFID tags are fitted to metal.
- After-market grips (Pachmayr) or grips containing a metal insert affect the performance of the RFID tag.
- The tag position on different weapons may possibly interfere with operation.
- Gun oil is likely to cause adhesion problems when fitting tags.
- GSM coverage and network availability for system updates and notifications.
- Charging the hand-held units for operation out in the field. Most devices have vehicle-charging capability, though electrical standards should be complied with for such electrical equipment within vehicles.
- The RFID tags have a short read range. However, this demands deliberate attention to an individual weapon to read the tag and avoids erroneous readings.

It is important that, wherever practicable, the RFID tag is fitted to the main body of the weapon on which the weapon serial number is marked. This ensures that the unique identifier stored in the tag always relates to an individual weapon's unique serial number to maintain the integrity of the database information. This is particularly important for some modern weapons which are modular in their construction and have interchangeable parts.

11 Conclusion

This project has met its objective and has proved that RFID technology can be applied to weapons issue and armoury management. This document can be used as a guide to good practice and the case study can be considered as an example to follow.

The project has demonstrated the feasibility of the technology to meet this particular application. However, it cannot be assumed that an off-the-shelf solution would suit all installations and that the performance of RFID tags is replicated when attached to different assets. Extensive testing in partnership with users and system integrators is highly recommended. Overall system compatibility with current police force infrastructure is encouraged wherever possible, taking into account individual police force requirements. In addition, thought should be given to possible force amalgamations or a national system being adopted in the future.

11.1 Lessons learned

- The advantages of developing a system in partnership with the end-user led to opportunities to enhance the performance of the system as it was developed, thereby improving integrity and functionality.
- Force IT Network relationship – though the case study installation was a stand-alone system, with the aim being that the Force IT Department would adopt ownership of the system, it was important to consult regularly with the department throughout the development. Certain security requirements had to be met, with the aim of full system adoption on to the network in the future.
- Identifying a suitable hand-held computer proved to be a difficult challenge. The aim was to find a ruggedised unit that had all the technology fully integrated within one product. For operational use, the unit had to survive a physical drop test, have RFID reading capability, have on-board Wi-Fi and GSM, and be as small as possible to be fitted within an ARV.
- Technology advancements – RFID as a technology is not new. However, applying the technology to weapons and armoury management is unique. Over the period of the project, technology moved on and though the aim was to use readily available hardware, there is no guarantee that manufacturers will not amend their product lines. For example, the model of hand-held computer used in this case study is no longer made by the manufacturers.
- It was noted that officers with particularly large hands had a different grip (Pachmayr) fitted to their handgun. It was found that this alternative, non-standard grip had metal reinforcements, causing problems in reading the RFID tags.

11.2 Recommendations

- Ideally, tags fitted at the point of weapon manufacture are preferred to retrospective fitting. Conclusive tests would need to be carried out on retrofitted tags to ensure that tag-reading performance is maintained. Retrospective gluing of tags to the surface of weapons, where gun oil is always present, is unavoidable and is not ideal.
- Stand-alone systems should be supported with a parallel system to be used as a test bed. This provides a confidence check to test any updates or maintenance upgrades and reduces the risk of adverse effects to a 'live' system.
- Built in to the system should be the contingency to revert back to a paper-based recording system at any time in the event of a system failure. Ensuring that data can be entered retrospectively maintains a seamless audit trail.
- Where other forces already have access control for their armoury, it may be possible that an armoury and weapons management system could be integrated into an existing system.
- Further investigation is required to identify a suitable hand-held computer to replace the obsolete models used in the case study.

11.3 Possible future developments

Through the development of the project and input from the users, there have been a number of suggestions that would generate further management benefits and technical improvements, such as:

- Central reporting to the relevant authorities, e.g. H.M.I.C.
- Direct reports on weapons faults to the Home Office Scientific Development Branch, Firearms and Protective Equipment Programme.
- Additional add-on software modules to include officer training and central incident management information.
- With the aid of the weapon manufacturers, RFID tags could be fitted at the point of weapon manufacture.
- Other equipment or valuable assets could be tagged and introduced into the system.
- Further investigation is required to identify an alternative RFID tag size and shape that would be better suited to be fitted to the range of police firearms and equipment.

11.4 Partnership working

This demonstrator system was developed in a partnership between HOSDB, Hertfordshire Constabulary and Innovate 21 as the system integrators.

The author wishes to acknowledge the valuable input from Sergeant Andy Knowles, Training Co-ordinator (Firearms), Hertfordshire Constabulary.

11.5 Contact details

Graham Dean
Home Office Scientific Development Branch
Sandridge
St Albans
Hertfordshire AL4 9HQ

Tel. 01727 816434

Fax. 01727 816420

Graham.Dean@homeoffice.gsi.gov.uk

Appendix A: The user’s operational requirements

The table below incorporates the Firearms Support Unit’s initial operational requirements with a description of how the system has been developed to meet those requirements.

The operational requirements are split into three main sections:

- A1 Implementing Security.
- A2 Weapons/Ammunition.
- A3 Training.

Each section outlines the business function aim and the function objectives , followed by a list of individual requirements as set out by the User.

User’s Operational Requirements	Description of how the Project met the Operational Requirements
A1. IMPLEMENTING SECURITY	
Business Function Aim	
<p>A high level of security is required in all aspects of the Firearms Department. There is, therefore, a need to have the ability to generate a unique ID for each authorised firearms officer (FOID) and for this ID to be the only way to access the armoury. Further to this, it will also be necessary for each weapon to carry a unique ID (WID).</p>	
Function Objectives	
Create a unique firearms officer’s ID (FOID).	Each authorised firearms officer (AFO) is issued with an RFID card that holds a unique electronic code.
Create a unique weapon ID (WID).	Each weapon is fitted with a uniquely coded RFID tag that is associated with the weapon’s serial number.
Create individual authorisation ID (AID) levels.	The system administrator assigns levels of access and authorisation to each officer.
Integrate an armoury entry system.	Entry to the armoury is only via the access control system.

A1.1 FIREARMS OFFICERS UNIQUE ID (FOID)

Association of unique ID with a firearms officer.

Business Function Aim

It is a fundamental requirement of the new system that it is able to take a unique ID and associate that ID with a given police officer. The unique ID cannot solely rely upon an officer's Warrant Card number, as over a period of time these are re-issued. It is therefore necessary for the unique ID to be at least a part of a series of information.

Function Objectives

A1.1.1 Unique ID

Each firearms officer ID (FOID) must be unique. There must be no duplicates within the system.

Each AFO's RFID card is manufactured with a unique electronic code. AFO identity is verified with a self-selected PIN. One card is issued per AFO and no duplicates are permitted.

A1.1.2 ID Acceptance

The system must be able to accept a new FOID and associate this to an AFO.

The administrator can add a new AFO to the system and associate their name, service number and RFID card to an FOID.

A1.1.3 Single FOID per user

It is essential that the system associates only a single FOID with each user at any one time.

Only one RFID card can be associated with each AFO. Duplicates are not permitted. Any discrepancies will raise an 'Unknown Card' alert.

A1.1.4 Replacement FOID for an Officer

The system must be able to issue a replacement FOID to an officer.

The administrator can issue a replacement RFID card to an AFO. The issue of a replacement card renders any previous cards void.

A1.1.5 Removal of FOID

The system must be able to accept the removal of an FOID and therefore the removal of an officer's authorisation to either enter the armoury or be issued with a weapon.

Administrator function allows an officer to be made 'unauthorised' instantly, preventing the card being used to log-on to the system or to access the armoury.

A1.1.6 Grading of FOID

The system must be able to associate each FOID with one of the four levels of system access.

It was acceptable for the Administrator to set authorisation level for:

Access to functionality of management computer and hand-held computer.

Access to armoury.

Weapon type issue authorisation.

A1.2 WEAPON ID (WID)	
Associating a WID with a weapon.	
Business Function Aim	
It is a fundamental requirement of the system that each weapon held by the police force is issued with a unique WID.	
Function Objectives	
A1.2.1 Unique ID	
Each WID must be unique.	Each weapon RFID tag has a unique electronic code.
A1.2.2 WID Acceptance	
The system must be able to accept a new WID and associate this to a given weapon.	The administrator can add a new weapon RFID tag to the system and associate it to the weapon's serial number.
A1.2.3 Single WID per Weapon	
It is essential that the system will only associate a single WID with each weapon at any one time. However, if the weapon's WID is replaced, the system must be able to show a complete history including all WIDs that have been associated to the item. The user must also be able to carry out a search on a weapon's history report for any WID.	The system associates a weapon's unique serial number with a unique electronic code within the weapon's RFID tag. In the event that a weapon's tag is replaced, the administrator can allocate a new tag to the same weapon. A log of this event is recorded in the weapon's history report.
A1.2.4 Replacement WID for a Weapon	
The system must be able to issue a replacement WID for a weapon. This can only be done under one circumstance and that is when the existing WID has been damaged. Administrator privileges will be required for this task.	The administrator can allocate a replacement tag to a weapon. The event is logged in the weapon's history report.
A1.3 ARMOURY ENTRY SYSTEM	
Business Function Aim	
It is a fundamental requirement of the new system that it restricts entrance to the armoury to authorised personnel only. Also note that it will be a further requirement of the system that each user MUST have entered the armoury via this system in order for the weapons' authorisation to work. All FOIDs will be stored on the system's database.	AFOs must use their RFID card plus a self-selected PIN to enter the armoury. Each entry attempt is logged in the system database.

Function Objectives

A1.3.1 ID Check

The system must be able to check the FOID of each user attempting to enter the armoury. NOTE: If the FOID is invalid then entry to the armoury MUST be refused.

When an AFO presents their card to access the armoury, the system verifies their status. Each successful and failed attempt to enter the armoury is logged, along with a captured image.

A1.3.2 Authorisation ID Check

The system must be able to check whether an officer is currently suspended from firearms duties. This is done through checking the officer's authorisation ID (AID). NOTE: It may be possible for the FOID to pass its check but for the AID check to fail, thereby refusing access to the armoury.

Each time an officer presents their card, the system checks validity. The system administrator can manually make any officer 'unauthorised' at any time, thereby refusing access to the armoury using their FOID card.

A1.3.3 Log Access Attempts

The system must log all access attempts to the armoury and store this information for a period of at least six months. The user will have a maximum of three log-in attempts before a set action is taken.

The system logs all attempts to enter the armoury along with an associated digital photograph. Successful entries remain on the system for 90 days. Unsuccessful attempts remain on the system indefinitely. Three attempts at card + PIN entry are permitted before lockout that requires a reset by an administrator.

A1.3.4 Back-up Entry System

A secondary entry system must be in place in case of primary failure. This system must also be able to check the FOID of the user attempting to enter the armoury. NOTE: If the FOID is invalid then entry to the armoury MUST be refused.

The access control system has local battery back-up in the event of power failure. In the event of total power loss, the system can revert back to manual key operation under previous key management procedures.

A2. WEAPONS/AMMUNITION

Business/Function Objectives

Detailed information about each weapon, its ammunition and usage must be maintained by the system. This information must be able to be checked, printed and collated into reports. These reports must adhere to 'Protective Marking' criteria.

A2.1 WEAPON SET-UP

Association of unique weapon ID with each individual weapon.

Function Aim

It is a requirement of the new system that it is able to associate a unique weapon ID with each unique weapon serial number.

Function Objectives	
A2.1.1 Weapon Type	
<p>The new system will be required to generate a template for each new weapon type. This must contain all relevant information associated with that weapon type, e.g. serial number, calibre, number of rounds held in weapon, along with trigger information for weapon maintenance.</p>	<p>Administrator function allows weapon types to be entered with their associated properties: serial number, make, model, ammunition type, authorisation level and maximum rounds fired before maintenance.</p>
A2.1.2 Add a New Weapon	
<p>The new system will be required to allow the addition of new weapons. Each new weapon must be associated with a weapon type and its WID.</p>	<p>Administrator function allows a new weapons serial number to be entered onto the system and associated with an RFID tag.</p>
A2.1.3 Archive a Weapon	
<p>The new system will be required to allow the deletion of a weapon from the armoury stock register. This information should not be totally removed from the system but placed in an archived section where it should be retained indefinitely.</p>	<p>Administrator function can mark weapons as disposed of. Such weapons still remain on the system and a specific list of disposed weapons can be generated in management reports.</p>
A2.1.4 Edit Weapon Details	
<p>The new system will be required to allow the user to edit weapon details. This should be restricted to administrator level access.</p>	<p>The administrator can edit weapon details.</p>
A2.2 ISSUING OF WEAPONS	
Function Aim	
<p>It is a requirement of the new system that it enforces security protocols associated with the issuing of firearms upon the user and records all relevant data.</p>	
Function Objectives	
A2.2.1 Link FOID to WID	
<p>The new system will be required to link each WID to the receiving officer's FOID. The system must check that the receiving officer has the correct authorisation to use the weapon.</p>	<p>The system administrator allocates weapon type authorisation levels to each AFO.</p>
A2.2.2 Weapon Status	
<p>The new system will be required to record the current status of each weapon, ammunition used, ammunition issued on each day and to which officer the weapon has been issued.</p>	<p>Weapon or Officer History Reports can be run to provide these details.</p>

A2.3 VEHICLE ARMOURY

Function Aim

It is a requirement of the new system that it is able to monitor all weapons held by the police force, including those held in the Armed Response Vehicles (ARVs).

Function Objectives

A2.3.1 Allocate Weapons to Vehicle

The new system will be required to allocate several weapons and ammunition to each ARV and monitor their usage. As part of the audit trail history, the issuing officer's details must be noted against the ARV.

An ARV is classified as a location and weapons can be associated to, and added to or moved from, the ARV in the same way as from a fixed armoury.

A2.3.2 Replace Weapon in Vehicle

The new system will be required to allow the replacement of firearms or change of weapon type and ammunition in the ARV.

Weapons can be replaced in the ARV by following the same process as for a fixed armoury.

A2.3.3 Issuing an ARV

The new system will be required to make all relevant security checks when issuing an ARV to an officer. (Identical to the checks undertaken when issuing a weapon.)

ARV issue follows the same process as a fixed armoury issue.

A2.3.4 Issuing Weapons to Officers in an ARV Whilst on Call

The new system will be required to monitor the issuing of weapons from the ARV whilst in the field.

Data collected from off-site or ARV issues are transmitted back to HQ as soon as transactions are completed, to provide near real-time monitoring information.

A2.4 AMMUNITION

Function Aim

It is a requirement of the new system that it is able to monitor all ammunition held by the police force, including those held in the ARVs.

Function Objectives

A2.4.1 Add Ammunition to Armoury

The new system will be required to allow the addition of ammunition to the armoury. Administrator level of clearance will be required.

The system allows complete ammunition stock control; only users with administrator level access can monitor and control stock levels, both incoming and outgoing.

<p>A2.4.2 Ammunition Type</p> <p>The new system will be required to generate a template for each new ammunition type. This must contain all relevant information associated with that ammunition type, e.g. calibre, type, amount, cost etc.</p> <p>A2.4.3 Allocate Ammunition to an Officer</p> <p>The new system will be required to monitor what ammunition is allocated to each officer and whether or not it is appropriate for the weapon issued.</p> <p>A2.4.4 Delete Ammunition</p> <p>The new system will be required to allow for ammunition data to be deleted. Administrator level of clearance will be required.</p> <p>A2.4.5 Edit Ammunition Levels</p> <p>The new system will be required to allow for ammunition data to be edited, i.e. increase/decrease levels due to use or stock order. Administrator level of clearance will be required.</p>	<p>Administrators can edit existing information and add new ammunition types onto the system, but cost information is not provided.</p> <p>Ammunition type and quantities are allocated by the system during the issue process to match the weapon type being issued at the time.</p> <p>Administrators can add or delete ammunition data.</p> <p>Administrators can modify ammunition data.</p>
<p>A2.5 RECORD MAINTENANCE</p> <p>Function Aim</p> <p>It is a fundamental requirement of the new system that it is capable of providing several reports and monitoring the maintenance guidelines set up for each weapons type.</p> <p>Function Objectives</p> <p>A2.5.1 Weapons Maintenance</p> <p>The system must be able to monitor the current status of each weapon and automatically prompt the user as to when it requires maintenance.</p> <p>A Weapons Due for Maintenance Report lists all weapons that need maintenance within their specified maintenance routine. There are four reports: weapons due now, weapons within 10% of maintenance, weapons within 20% of maintenance, and weapons within 50% of maintenance.</p> <p>A2.5.2 Armoury Status</p> <p>The system must be able to provide an instant report showing the current status of the armoury, displaying the weapons and ammunition issued, and to whom they were issued.</p> <p>Current status reports can be generated to show total armoury inventory, or individual weapon or officer history at any given time. Ammunition usage and stock management reports can be produced.</p>	

A2.5.3 Stock Levels

The system must be able to provide a report of all stock levels within the armoury and prompt the user as to when certain stock needs replenishing.

The system can list an inventory of weapons and ammunition to the administrator. No prompt is generated for stock replenishment, but it is thought that this would be feasible with further development.

A2.5.4 Search Facility

The system must allow the user to undertake searches on an officer's name, WID or FOID.

Searches and reports can be generated based on AFO name and service number or weapon serial number.

A2.5.5 Weapon History

The system must be able to provide a complete history of a weapon: ammunition fired, by whom and last maintenance date (all events concerning the weapon).

Reports can be generated to provide all aspects of a weapon's history.

A2.5.6 Display Weapons

The system must be able to provide a complete breakdown of all weapons that are held within the armoury for display purposes.

Only operational weapons are tagged in this project. Display weapons are not tagged, but this is feasible.

A2.5.7 Returned Weapons

The system must be able to provide a listing of all weapons handed in by members of the public and the action taken in respect of that weapon, i.e. destroyed, placed in display etc.

This is feasible, but is not included in this project.

A3. TRAINING

Integration of training data.

Business/Function Objectives

All training information is currently recorded on the dedicated Human Resources (HR) system, for which there are discussions underway regarding the possibility of developing a direct interface to the new system. This will eliminate the need for duplication of work when updating records.

All of the above requirements were considered as essential requirements. The following user requirements applicable to this Training section were considered as 'Desirable'. On-going developments are underway to attempt to integrate Training and HR details into the armoury management system.

A3.1 Maintaining Information

Record generation and data monitoring.

Function Aim

It is a requirement of the new system that it is capable of reading and recording information to the HR system.

Function Objectives

**A3.1.1 Reading Training Information
[Desirable]**

The system must be able to allow searching of training information held within the HR system.

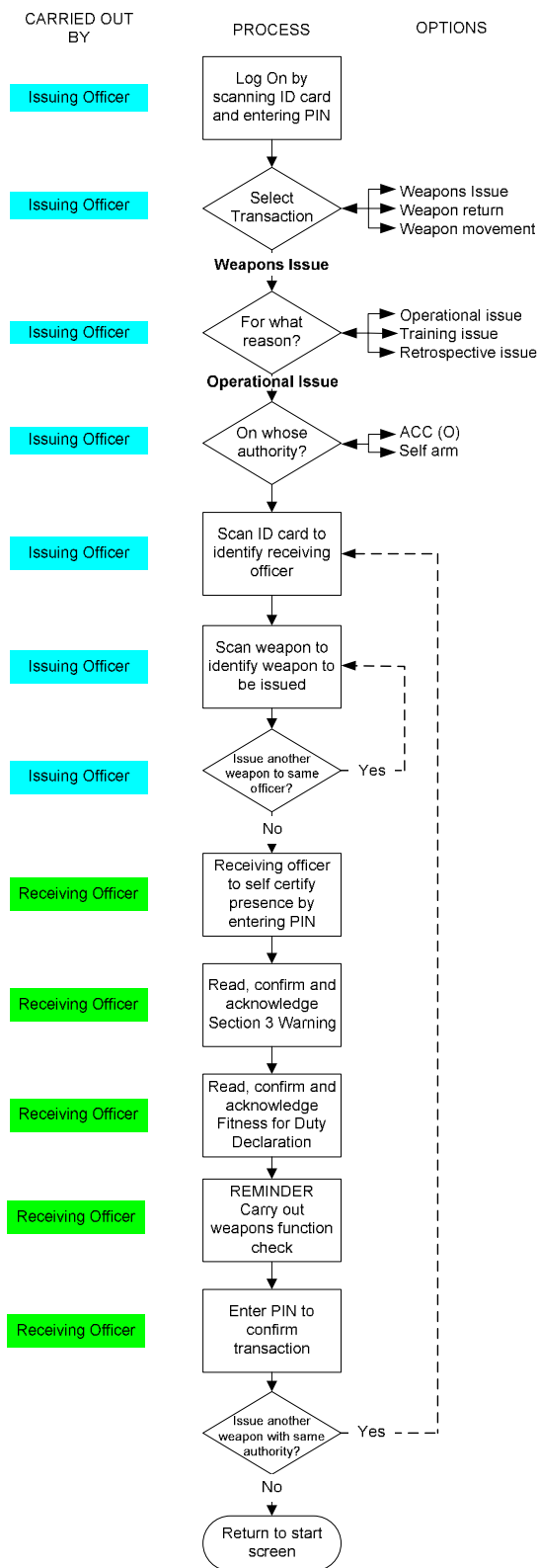
**A3.1.2 Updating Training Information
[Desirable]**

The system must be able to allow the updating of training information held within the HR system. Some of this information may need to be recorded on the new system, with regards to weapons and ammunition used.

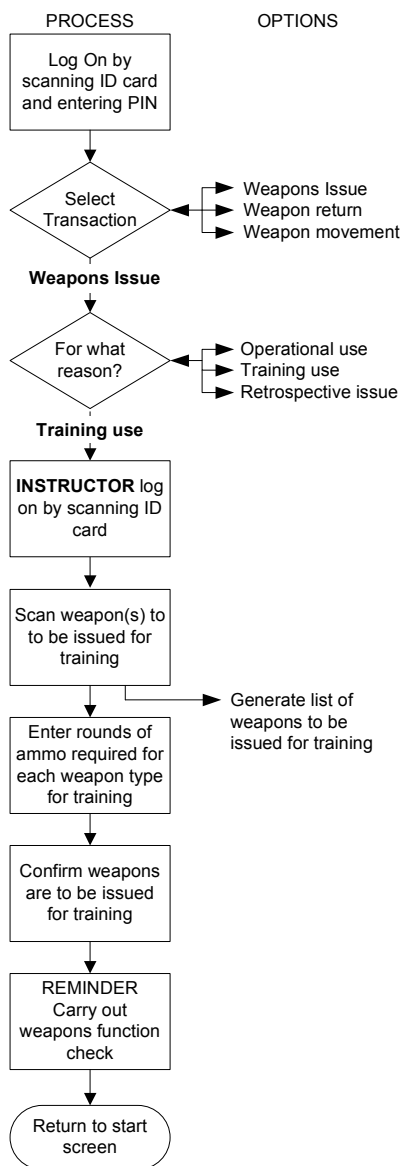
**A3.1.3 Locking Training Details
[Desirable]**

The system must be able to allow the locking out of training information held within the HR system. This information must then be accessible only to users with administrator level clearance.

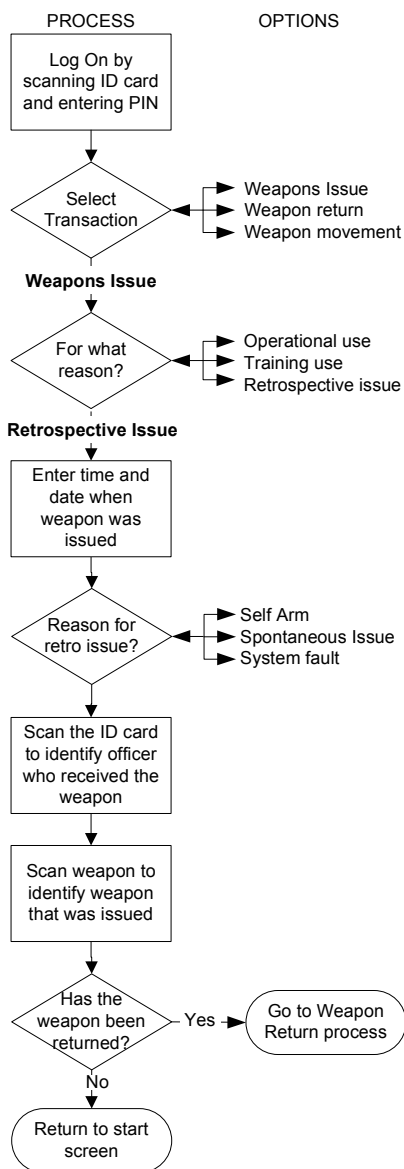
Appendix B: Process flowchart – weapons issue for operational use



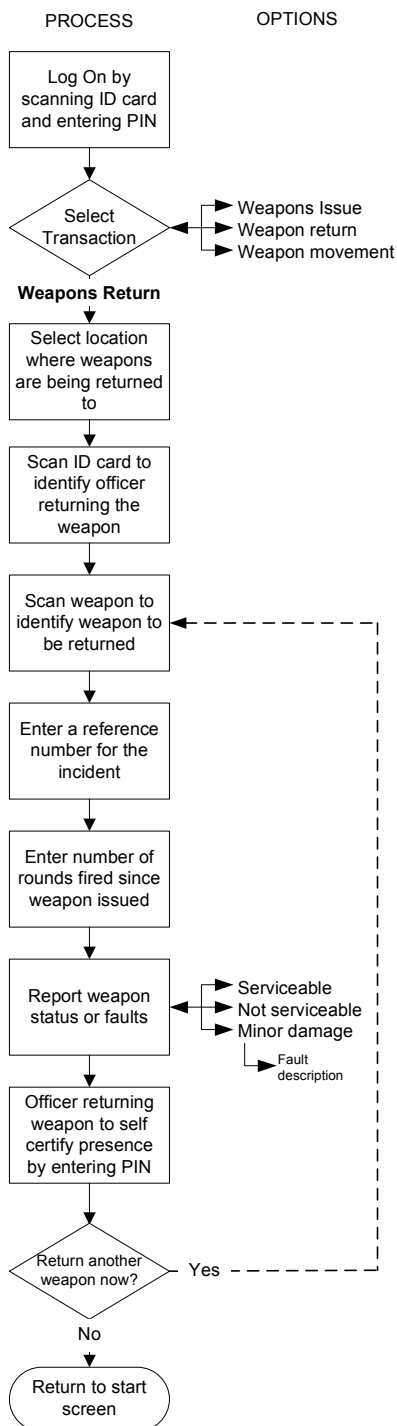
Appendix C: Process flowchart – weapons issue for training



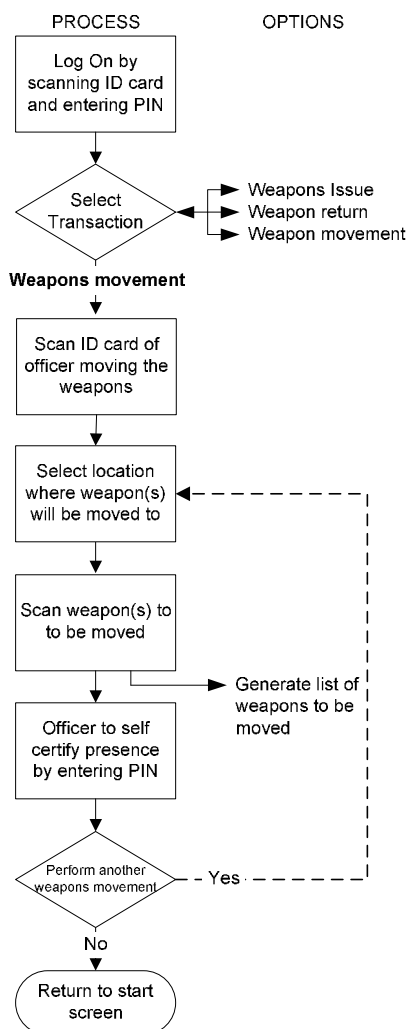
Appendix D: Process flowchart – weapons issue retrospectively



Appendix E: Process flowchart – weapons return




Appendix F: Process flowchart – weapons movement



Appendix G: Glossary of terms

ACPO	Association of Chief Police Officers
AFO	Authorised Firearms Officer
AID	Authorisation Identification
ARV	Armed Response Vehicle
FOID	Firearms Officer Identification
GSM	Global System for Mobile communication, i.e. mobile phone network
HOSDB	Home Office Scientific Development Branch
ID	Identification
ISDN	Integrated Service Digital Network
IT	Information Technology
PCA	Police Complaints Authority
PIN	Personal Identification Number
RFID	Radio Frequency Identification
SIM	Subscriber Identity Module e.g. mobile phone SIM card
SMS	Short Message Service
TSV	Tactical Support Vehicle
URN	Unique Reference Number
Wi-Fi	Wireless Communication (or Local Area Network or 802.11b)
WID	Weapons Identification
UK	United Kingdom



Home Office Scientific Development Branch
Sandridge
St Albans
AL4 9HQ
United Kingdom

Telephone: +44 (0)1727 865051

Fax: +44 (0)1727 816233

E-mail: hosdb@homeoffice.gsi.gov.uk

Website: <http://scienceandresearch.homeoffice.gov.uk/hosdb/>