
ANNEX R-3 OF SCHEDULE R**LIVESCAN FUNCTIONAL REQUIREMENTS SPECIFICATION**

The Livescan Functional Requirements Specification contained within this Annex reflects the current provision of Livescan as at the Effective Date. Both Parties acknowledge however that this Annex R-3 document will need to be updated to incorporate and reflect agreed changes in the Livescan functional requirements as a result of the Contractor fulfilling its on-going obligation to meet Schedule D (**Detailed Operational Requirements**) of the Contract. It is furthermore agreed between the Parties that at FOC, the Livescan Functional Requirements Specification will be fully updated to include all agreed changes (including but not limited to functionality) and submitted as part of the acceptance procedures in accordance with Schedule H (**Acceptance Procedures**).

CONTENTS

1	INTRODUCTION.....	1
2	REFERENCE DOCUMENTS	2
3	OVERVIEW	3
4	REQUIREMENTS.....	24
	APPENDIX A - LIST OF ACRONYMS.....	42
	APPENDIX B - GLOSSARY OF TERMS	44

LIST OF FIGURES

FIGURE 3-1 LIVESCAN HIGH-LEVEL ARCHITECTURE	3
FIGURE 6-2 TOP LEVEL CHARGING STATION PIC PROCESSING	5
FIGURE 3-1 TEN PRINT CAPTURE PROCESS.....	18

LIST OF TABLES

TABLE 3-1 USER ROLES.....	10
TABLE 3-2 TEN PRINT LIVESCAN SUBMISSION DATA ITEMS	18
TABLE 0-3 LIVE-ID REQUEST DATA ITEMS	19

1 INTRODUCTION

The IDENT1 Charging Station Segment, a segment of the IDENT1 Operational System, is designed to provide the Police Forces of England and Wales with remote identification products, located primarily in a Police Custody Office. Remote refers to the fact that they are outside of the IDENT1 Bureau or Central Segment location. The Charging Station Segment includes products and services such as Livescan, Live-ID, Interface Services, Mugshot Systems, etc. This document specifies the detailed design of the IDENT1 Livescan Subsystem (ILSS), a Subsystem of the Charging Station Segment.

1.1 Scope

This Functional Requirements Specification was created based on an analysis of the needs of the Police Forces of England and Wales and provides the detailed design of the IDENT1 Livescan option to IDENT1. This document is intended as a design specification and reference guide for Northrop Grumman project personnel, and Livescan vendors.

1.2 Purpose

The purpose of the *IDENT1 Livescan Functional Requirements Specification* is to document the system concept and functional requirements used to provide the basis from which the IDENT1 Livescan design can be validated.

1.3 Document Organisation

The Livescan Functional Requirements Specification contains the following sections:

Section 2, References, provides a list of documents with direct relevance to this document.

Section 3, Overview, presents an overview and concept of operations for the IDENT1 Livescan Subsystem.

Section 4, Requirements, provides the detailed requirements for IDENT1 Livescan, including Northrop Grumman "Cardinal" Requirements.

Appendix A - List of Acronyms, provides the definition of acronyms used within this specification.

Appendix B - Glossary of Terms, provides definitions for the terms used within this specification.

2 REFERENCE DOCUMENTS

Document	Document Number	Author	Date Issued
IDENT1 Livescan Interface Specification		Northrop Grumman	
NSPIS Custody to IDENT1 Livescan Interface Concept of Operations		Northrop Grumman	
NSPIS Custody to IDENT1 Livescan Interface Control Document		Northrop Grumman	

3 OVERVIEW

3.1 Livescan Overview

Livescan is one of the subsystems within the Charging Station Segment. These subsystems provide the Custody Staff at local police stations (or custody offices) with a suite of hardware and software that reduces the manual effort required currently for the reporting or charging of persons in custody.

The Livescan Subsystem comprises hardware and software components located in two physical locations, as illustrated in Figure 3-1. The Livescan Workstation is located in the Custody Office. Also located in the Custody Office is a router used to connect the Livescan Workstation with a IDENT1 Fingerprint Bureau. The Livescan Subsystem includes a Livescan Store and Forward device and Livescan printer that are located physically at the Fingerprint Bureau so that hardcopy Ten Print forms can be printed at the Fingerprint Bureau. Also, the Livescan Store and Forward submits Ten Print forms electronically to the IDENT1 Bureau Front-End Subsystem.

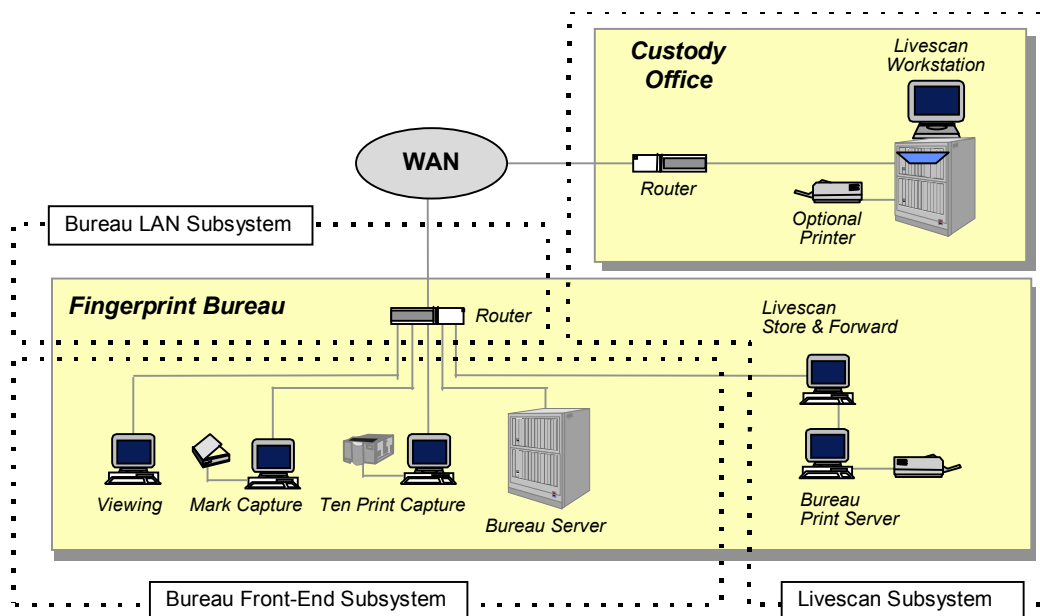


Figure 3-1 Livescan High-Level Architecture

Livescan provides a means of capturing electronically all rolled impressions, plain impressions, and palm prints directly from an individual's hands without the use of ink. The hand or individual fingers are placed directly on a camera platen that captures the fingerprints, producing digital images. The images are then processed in real time to produce immediate quality feedback to the user. Once the capture process is completed, including any entry of demographic data, the images can be transmitted electronically to a IDENT1 Fingerprint Bureau (or the NFO) for Tenprint Submission processing, a Live-ID Identity Check (Print-to-Print) or a Print-to-Mark Crime Check. In addition, the images and textual data may be printed out at the Fingerprint Bureau to produce standard IDENT1 Ten Print forms.

3.2 IDENT1 Livescan Subsystem Concept of Operations

This section describes the Concept of Operations (CONOPS) for all the capabilities of the IDENT1 Livescan Subsystem (ILSS), including electronic Ten Print capture, electronic Ten Print submission, Live-ID, and system management. This section was created based on an analysis of the needs of the Police Forces of England, Wales, and Scotland. The CONOPS is a reference guide for Northrop Grumman project personnel, as it documents the IDENT1 Livescan option and its operating capabilities from which the design and development is based. The analysis included information gathered during site visits to the Forces, discussions with the Authority and with Livescan vendors and other applicable IDENT1 documentation.

The purpose of the CONOPS is to document the operational capabilities of IDENT1 Livescan from a user perspective at the Custody Office. It is intended to document, at a high level, the operational capabilities and the transactions (or threads) IDENT1 Livescan will support. It will provide the basis from which the design and development can be validated.

3.2.1 Charging Station PIC Processing

This section describes the steps involved in processing an arrested person (Person in Custody (PIC) or Detainee) at a typical Custody Office from the point of view of interacting with IDENT1 Livescan. Figure 3-2 contains a diagram representing this process, with the bolded boxes representing processes involving Live-ID or Livescan.

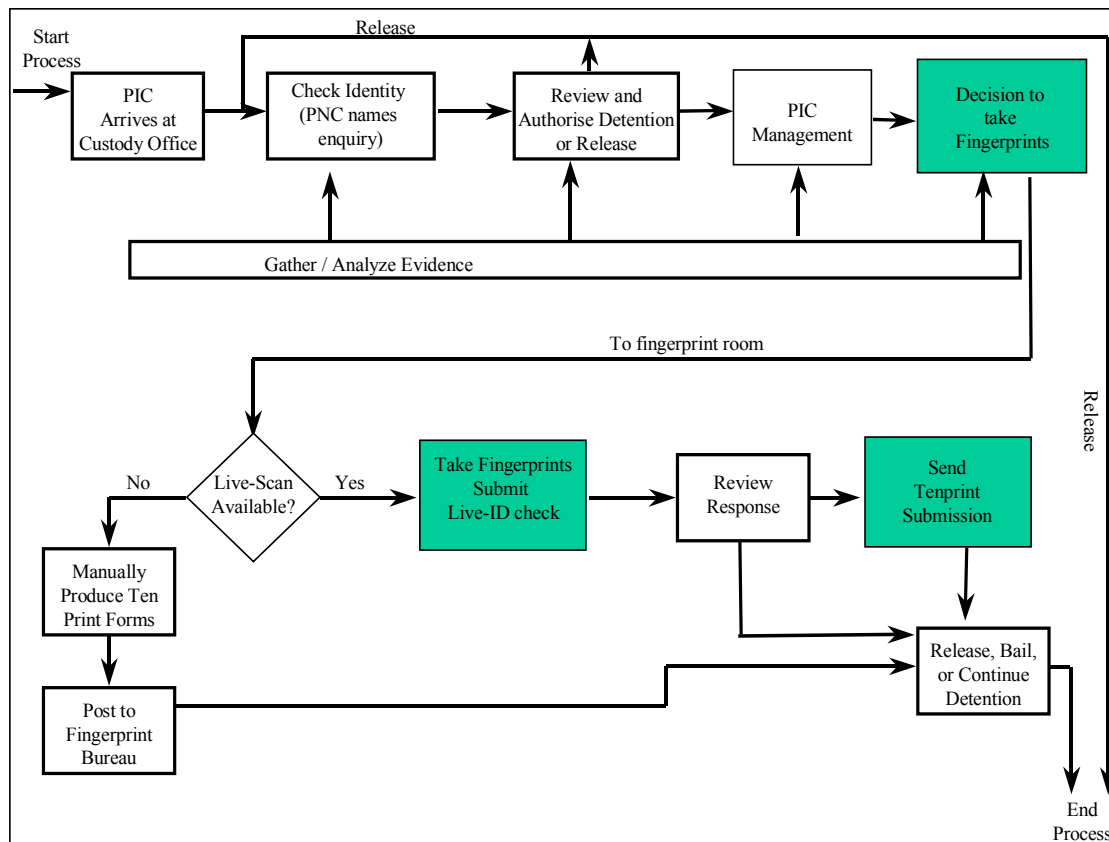


Figure 3-2 Top Level Charging Station PIC Processing

The process begins when the arrested person (or PIC) is brought to the Custody Office and presented to the Custody Staff by the arresting police officer. The reason for the arrest is discussed with the Custody Staff, who then makes a decision whether to release immediately the person or continue the process. If not released immediately, the PIC is searched and his or her possessions are confiscated.

The next step is to check the identification of the PIC for the purpose of verifying his/her correct identity. This is a critical step in the processing of the PIC, since incorrectly identifying a person in custody could result in that person being entered into the criminal justice system under a false identity. The process is begun typically by creating a custody record, either using an automated Custody System or by filling out a paper Custody Record form. The record is filled out initially using information received from the PIC. Next a PNC/Phoenix Name search is performed, and possibly other automated name searches, if these are available at the particular Custody Office.

Following these initial name searches, if the Custody Office is equipped with an IDENT1 Livescan Workstation, the PIC's fingerprints are captured electronically. This is a complete ten print set, including plain impressions and palm impressions as well as preliminary demographic and arrest information. Where an interface exists between a National Strategy for Police Identification Systems (NSPIS) Custody application (or other computerised custody system) and IDENT1 Livescan, demographic information is passed automatically to Livescan and a Livescan record created and cued ready for fingerprints to be taken.

Once the fingerprints have been taken, a Live-ID search can be initiated. The Live-ID Identity Check can be either a verified response or a non-verified response, as specified by the Livescan User. A verified response refers to search respondents that are verified by two separate Fingerprint Officers. The verified search results displayed to the Livescan User indicate a verified result, either Ident or Non-Ident. In the case of an Ident, one individual is listed, identified by the CRO number. When the search is specified as non-verified, an automated search of the IDENT1 national database is executed, returning typically from one to three CRO numbers with an identification confidence rating of 'high', 'medium' or 'low'. Livescan will retain and display a single CRO that is returned as a result of a Live-Id non-verified search responses. The returned CRO will be automatically input into the CRO field. The returned CRO Number of the individual can then be used by Custody staff to look up the complete criminal record in conjunction with PNC/Phoenix. Not only may the identity of the PIC be established, but useful information regarding PNC warning signals (escaper, contagious disease, assaults police, and the like) and also outstanding warrants for arrest can be ascertained. Therefore, it is desirous for the PIC to be fingerprinted and searched on Livescan as quickly as possible into the Custody process.

The Custody staff may elect to search the PIC against the Immigration and Nationality Directorate (IND) database at the Immigration and Asylum Fingerprint System (IAFS). Police Officers and other authorised Users are able to request IAFS searches from Livescan Workstations. The IND searches may be verified, non-verified, or use a quoted IFB reference number. When a response from a Livescan initiated search request to IAFS is accompanied by a digital photograph, the Livescan workstation displays the available digital photograph.

The IND search may return up to five Immigration Fingerprint Bureau (IFB) Numbers. The IFB search results may include IND contract information including the IND phone number, fax number, and electronic mail address of the IND officer. Additionally, the search results will include any available digitised photographs. The IFB numbers, contact information, and photographs are displayed on the Livescan Unit to assist with PIC identification. In response to a Livescan initiated search, two separate response messages will be sent to the Livescan workstation, one for the IDENT1 Live-ID request and one for the IAFS search request.

Additionally, a search of the unsolved Mark database at the local, regional, or national level is possible. The Print-to-Mark search can potentially identify a PIC who has been involved in an unsolved crime. The Print-to-Mark Crime Check is a verified search. The "verified" type routes to the local Fingerprint Bureau and is checked by three fingerprint officers before returning an "Ident" or "Non-Ident" response to the Livescan unit.

The PIC may be placed in a holding cell while waiting for the search results or continue to be interrogated while the Custody Staff fills out the Custody Record. The arresting police officer also begins the process of gathering and analysing evidence related to the crime. This may take place in parallel with the Custody Staff's processing of the PIC.

After the PIC's identity has been verified, the Custody Staff reviews the charges and formally authorises the detention or release of the person. If released without charge, the Ten Print record is forwarded to IDENT1 as an "arrestee" form type for filing and the process ends. If the detention is authorised, then the Custody Record is updated with the pertinent information.

If the PIC is charged, the record is electronically submitted to the Police Force's Fingerprint Bureau using the Tenprint Submission transaction on the Livescan unit. The relevant Arrest/Summons (A/S) Number is entered into the Livescan system, prior to making this Tenprint submission allowing IDENT1 to expedite the processing of the record. The Livescan transaction may also be updated with additional demographic and arrest data before

making the submission. (N.B. Where an interface exists between an NSPIS Custody application (or other computerised custody system) and IDENT1 Livescan, demographic information is passed automatically to Livescan. This normally includes the A/S number.)

The results from the Ten Print Submission to IDENT1 are received by the submitting Livescan workstation once the transaction has been verified at the IDENT1 Bureau. One or more copies of the fingerprint form is always printed at the IDENT1 Bureau receiving the submission.

Following either the Livescan ten print submission or the manual fingerprint taking, the decision is reviewed whether to release, bail, or continue to detain the person. Finally, the Custody record is closed out when the person is released.

The Ten Print record held on the Livescan workstation will be automatically deleted by the system once it has been transmitted to IDENT1 and successfully closed out at the end of IDENT1 processing. In addition, the Livescan record may be deleted at any point in the process by authorised Custody staff. This may be necessary in rare circumstances, such as wrongful arrest. (N.B. Deletion actions are fully audited by the system.)

3.2.2 IDENT1 Livescan User Community

The users of IDENT1 Livescan are comprised mainly of the Police Force operational personnel, support personnel and administration staff who operate within, or for operational reasons, visit a Custody Office. The Custody Office is a physically secure environment intended to restrain the movements of persons in custody. The IDENT1 Livescan terminals, equipment are normally located within this controlled area. Day to day access, therefore, is restricted in the first instance to personnel authorised to enter the restricted area of the Custody Offices and then to those who have been designated, trained, and entered into the system as authorised users. A second set of users, those who only require access on a limited and non-scheduled basis, consists of the maintenance personnel who repair hardware or software problems (Northrop Grumman personnel) and administrative users who collect processing statistics. Northrop Grumman maintenance personnel may connect as available, through communications links to the equipment via the IDENT1 central segment.

3.2.2.1 Primary Users

Those with direct contact with the equipment consist of the Custody Staff taking the information and capturing the fingerprints, and the PIC whose prints are being taken.

- Custody Officer. The Custody Officer (often a Custody Sergeant) has a legal responsibility to control the physical access to the restricted Custody Office area and is responsible legally for all activity occurring within the Custody Offices. The Custody Officer is responsible also for all the equipment within the Custody Office area. A Custody Officer is a fully trained user of the system for the taking of fingerprints for both identification purposes and for submission of the full ten print sets. However, the Custody Officer would normally delegate the task to a Custody Office support staff or jailer, because of the independent and impartial responsibilities placed upon the role by the Police and Criminal Evidence (PACE) Act legislation. The Custody Officer may require access to system audit trails or information on the capture and transmission of data for statistical or evidential purposes. The responsibility for such tasks varies from Police Force to Police Force. Where an interface exists between an NSPIS Custody application (or other computerised custody system) and IDENT1 Livescan, the Custody Officer may select to create a

record on the IDENT1 Livescan unit, cue for fingerprinting, and request a particular search type (e.g. Live-ID non-verified), direct from the Custody application.

- Custody Officer Support Staff. With the exception of the smallest stations, the Custody Officer will have a support staff, which may be regular police officers, referred to as a Detention Officers or Jailers. A civilian or an unpaid Special Constable may also undertake this role. The support staff are the main users of the system and routinely take the fingerprint images of the PIC under the direction of the Custody Officer. The support staff is restricted to the routine taking and transmission of the fingerprint images. Additional responsibilities may include minor administrative tasks that require access to the search results for previous transactions and to ensure that transactions have been fully completed. Tasks are also likely to include routine preventative maintenance, such as platen cleaning, fault reporting and general cleanliness of the equipment.
- Person in Custody (PIC). The physical movements of a PIC are restricted to the area within the secure perimeter of the Custody Office. All identification and submission transactions involving the PIC take place on equipment within the secure perimeter. The equipment is normally in an area dedicated to PIC administrative functions and the PIC is under constant escort while in that area. If the PIC is under-age, he or she may be accompanied by his or her legal representative, and, where the PIC is immature or mentally defective, by a Guardian or similar representative. However, these persons, if present, will have no contact with the equipment. Use of the equipment by a PIC is restricted to the following functions:
 - The provision of fingerprint images for identification or submission purposes.
 - The signing via a digital signature pad of fingerprints taken from the PIC.
 - The only use of the Livescan system that a legal representative or guardian of a PIC has is to observe the first of the two transactions listed above.

3.2.2.2 Secondary Users

Secondary Users are those who do not have direct day-to-day contact with the equipment.

- Trainer. The Police Force requires police trainers to be trained so that they have the capability to train local Custody Centre personnel in the use of Livescan.
- Indirect Users. A number of other officers within the local Police Station or Force may have need for information obtained from the IDENT1 Livescan System. Normally, this information is included as part of the Custody Record maintained on the individual, or as part of the Case Preparation maintained in conjunction with the Crown Prosecution Service (CPS). However, in limited cases the individuals may need to obtain information in a critical time period and may need to access the data at the source.
- Case Officer. The Case Officer is responsible for progressing all aspects of the case against a PIC to a successful conclusion, which often includes establishing the correct identity of the PIC. IDENT1 Livescan will provide these officers with information on the identity of the PIC. Some Police Forces may also require these officers to be trained users of the Custody Office System, in which case they would be functioning as Custody Staff Officers.

- Criminal Investigation Department (CID). A CID Officer may also be a case officer in the more serious cases. Otherwise, the role of the CID officer is often to assist Case Officers where the case is difficult or involves a serious category of crime. This type of user may make use of the identifications from the IDENT1 Livescan workstation.
- Scenes of Crime and Scientific Support. Specialists in the task of scientific support of the investigation of Crime are experienced in the collection of fingerprint evidence and its use. They may receive the results of fingerprint identifications performed using the IDENT1 Livescan workstation. They might use Livescan to capture elimination prints.
- Superintendent and Operational Inspector. The Police Superintendents and the operational Police Inspectors are ranks that have specific responsibilities under PACE legislation. Their consent and authorisation is required to perform certain acts such as to take fingerprints from a PIC by force. Both ranks are also likely to be the operational supervisors of Custody Officers and are responsible for overseeing the whole custody process. They also receive any complaints by PIC's. They access the system to determine, if possible, where malpractice has occurred. These individuals are most likely be looking at the statistical differences in the fingerprint capture; any deeper examination of records is the task of the IT specialist or Data Protection Officer.
- Police Force Statistics Officer. Additional management information required by the local Police Force on the management information and statistics captured and stored in the IDENT1 Livescan workstation requires access by the local Force Statistics Officer.

3.2.2.3 IDENT1 Livescan User Roles and Authorisations

There are two primary "User Roles" of the IDENT1 Livescan Subsystem. The first is referred to as a "IDENT1 Livescan User", corresponding to the typical user of the system, or Custody Officer or Support Staff. This individual does not possess "Manager" authorisations.

The second role is referred to as a "IDENT1 Livescan Manager". This individual is a more senior Custody Officer, or a more senior officer within the Force who has been designated to possess "Management" authorisations.

The third role is referred to as the "System Administrator" role. This individual performs system administrator functions. Table 3-1 contains the list of functions assigned to each user role.

Table 3-1 User Roles

User Role Name	Authorised Functions
IDENT1 Livescan User	Ten Print Capture Ten Print Submission Live-ID Print to Mark Search IND search
IDENT1 Livescan Manager	IDENT1 Livescan User functions, plus System Management Functions, including: Reports User Administration Local File Management
System Administrator	System Administrator functions

3.2.3 Functional Capabilities

This section describes the functional capabilities of the IDENT1 Livescan Subsystem. It contains subsections corresponding to the seven primary IDENT1 Livescan capabilities of ten print capture, ten print submission, identity check, crime check, immigration searches, 24-hour verification, and system management.

The Livescan User Interface options are:

- Electronic Ten Print Submission (verified search and full ten print processing)
- Live-Id (user option for verified or non-verified search)
- Print-to-Mark Crime Check (verified search)
- IND search (user option for verified or non-verified search)

3.2.3.1 Ten Print Capture

The IDENT1 Livescan subsystem provides electronic Ten Print capture capabilities. Using the IDENT1 Livescan workstation, ten rolled impressions, plain impressions, and palm prints (including the writer's edge) are captured by placing the person in custody (PIC) finger(s) or palm directly on a camera platen, which produces an electronic image of the fingerprints. There is also a capability to capture electronically the signature of the individual taking the prints. A straightforward Human Computer Interface (HCI) provides step-by-step operating instructions to the Livescan User.

The fingerprint images are displayed on a computer monitor, with the scanned image updated in real-time to provide a live video effect. This provides instant feedback to the Livescan user while the finger or hand is still on the platen. "Amputated" fingers or fingers "Not Taken" due to injury can be specified by the user through the HCI during the capture process, which is required by IDENT1 for proper classification and processing of the prints. During the capture process, extensive automated quality checks are performed and feedback is presented to the user to ensure that each image is of acceptable quality. The quality checks are described in more detail below.

The capture process also includes the entry of required demographic and arrest information, corresponding to the data entry items on the IDENT1 Ten Print Form. This data is entered directly through the Livescan workstation. Once the images and the demographic data are captured successfully, they are stored temporarily in the Livescan workstation until deleted by the user or automatically following a successful closeout of the record on IDENT1. An attempt to delete the local Ten Print record before it has been received and validated by IDENT1, will result in a warning message to the user.

Livescan Quality Checks

There are two general types of quality checks performed on the captured fingerprint images. The first is a check to determine whether the captured image is of sufficient quality, and occurs immediately after the image is captured. The specific image qualities analysed look at factors such as lightness or darkness of the image, the size of the image area captured, and image clarity. If an image falls below an overall threshold score, the user is notified immediately that it failed the quality check. He or she has two choices, they are:

- Make another attempt to capture the image, or
- Over-ride the warning and accept it. Override is only available following a second attempt.

If the user chooses to over-ride the quality warning, the system will record this fact in the audit trail.

The second quality check ensures the proper sequence of the fingers (i.e., that captured finger one is actually the right thumb). This is accomplished by a fast auto-encoding of the images and then performing a comparison of the rolled impression with what should be the corresponding plain impression. Any mismatches are reported to the user.

Users should be reminded that the automatic checks are not a substitute for good training and continued care and attention during capture, which are essential to the maintaining of good quality images to enable the continued effectiveness of fingerprint identification.

Demographic Data Entry

Demographic and arrest data may be entered either at the time of creating the record on the Livescan workstation, or after the fingerprint capture process has taken place. In order to best meet the needs of individual forces, the setting of certain demographic fields to "mandatory" is implemented by IDENT1 system admin staff following consultation with each force. In practice, fields such as "surname", "A/S number", "date-of-birth", "custody number", etc. are usually set as mandatory. Where an interface exists between an NSPIS Custody application (or other computerised custody system) and IDENT1 Livescan, demographic information is passed automatically to Livescan and a Livescan record created and cued ready for fingerprints to be taken.

The Livescan HCI notifies the user when required data, depending upon form type, has not been entered at the time the user attempts to complete the transaction. Demographic fields that have a fixed set of choices display these choices in “pop up” lists that the Livescan user can choose from.

Form Types and Form Formats

The accepted IDENT1 Form Types that can be submitted from Livescan include “Arrestee” (charge or caution), “Charged”, “No Further Action”, and “Suspect”. The form type is selected through the Livescan HCI, which produces automatically the “Form Identification Number (FIN)” and the correct layout of the fingerprints and demographic data when printed on a pre-printed fingerprint form. An “Arrestee” Form Type is set as the default in a Custody environment, which the user can over-ride through a selection on the HCI.

The IDENT1 Livescan workstation supports a single default Form format for each Form Type. The Form Format specifies the positioning of the fingerprint images on the form. The definition of a new Form Format is considered a maintenance item that must be performed by the maintainers of the system.

3.2.3.2 Ten Print Submission

Once the Ten Print record has passed the automated quality checks and is accepted by the user, the Livescan user has the option of submitting the ten print record to IDENT1 to be searched against the National Collection and be added to the database (if necessary). The fingerprint images are compressed and combined with the demographic data into a formatted message. The rolled impressions are compressed using a JPEG lossless compression algorithm, while the plain impressions and palms are compressed using a JPEG lossy compression algorithm. The record is then transmitted to the designated IDENT1 fingerprint bureau for processing.

The ten print submission is processed as a standard ten print submission, within the standard time frames allowed by the IDENT1 Service Level Requirements (SLR). If a unique Criminal Records Office (CRO) Number is specified with the submission, the transaction is processed within IDENT1 as a quoted CRO Ten Print Submission. If a CRO Number is not included with the submission, or if the quoted CRO Number is determined to be a “Non-Ident”, then a cold search of the National collection is performed automatically. Once the Print-Print processing has been verified and the CRO assignment made within IDENT1, a response is sent back to the submitting Livescan workstation, indicating the results of the IDENT1 submission.

Local/Remote Printing

Each IDENT1 fingerprint bureau configured for IDENT1 Livescan is equipped with one or more Livescan printers capable of handling the Livescan printing load for that Force. (In addition, an optional local Livescan printer can be connected to the Livescan workstation at the Force to provide a local printing capability). A high quality laser printer prints the captured fingerprint images and demographic data onto pre-printed IDENT1 Ten Print Forms, along with a unique FIN that is printed on the Ten Print Form in bar code and human readable form.

3.2.3.3 Live-ID Identity Check

As an alternative to immediately submitting the entire Ten Print record to IDENT1, a Live-ID Identity Check can be initiated, that is intended to determine the identity of the PIC with a quick response returned from IDENT1 to the Livescan unit.

IDENT1 Livescan functionality enables the Livescan User to perform both a Live-ID search and a full Ten Print submission to IDENT1 using the same capture process and the same images. This eliminates the need to capture the prints more than once. Once the Ten Print record has been captured (fingerprint images and optionally the demographic and arrest data), a Live-ID search can be initiated, which will use ten of the rolled impressions to be compared against the matching CRO number or searched against the National Ten Print Collection.

The Live-ID Identity Check can be either a verified response or a non-verified response, as specified by the Livescan User.

Verified Search Request

A verified response refers to search respondents that are verified by two separate Fingerprint Officers. The verified search results displayed to the Livescan user indicate a verified result, either Ident or Non-Ident. In the case of an Ident, one individual is listed, identified by the CRO number. This function provides a means of establishing a positive identification of a PIC at the start of the custody process, potentially saving a great deal of time and energy attempting to determine his or her identity using other methods. It may save time by eliminating the entry of false information, as well as preventing a person from being released after giving false demographic details.

The user can request a Live-ID Identity Check with a quoted CRO, which is a one-to-one comparison performed against a specific individual already in the National Collection. The search results are checked by two Bureau fingerprint officers. The system automatically performs a Cold Search of the entire National Collection if the one-to-one comparison results in a "Non-Ident" response. Livescan processing of a Quoted CRO compares the respondent CRO with the retained Quoted CRO. A match/mismatch indicator is displayed to the Livescan user.

Where any doubt exists in the mind of the Custody Officer following a Live-ID verified result, then a full Ten Print Submission should be run in order to get a confirmed result from the Fingerprint Bureau.

Non-Verified Search Request

When the search is specified as non-verified, an automated search of the IDENT1 national database is executed, returning typically from one to three CRO numbers with an identification confidence rating of 'high', 'medium' or 'low'.

The non-verified response refers to the fact that a FPO does not verify the results of the AFR search. Instead, results come directly from an automated search conducted by IDENT1. The results are displayed to the Livescan user in the form of between one and three CRO numbers.

To assist the user in determining the likelihood of a respondent being correct, a "Confidence Level" is displayed for each (non-verified) respondent. The confidence level, which is based on the score computed by the IDENT1 AFR Matcher, is displayed as "High", "Medium", or "Low". It indicates the probability of that respondent being an actual match. The

confidence level thresholds are configured at the IDENT1 central site. The confidence level can assist in determining the individual's identification, especially when used in conjunction with other systems, such as a Mugshot System or PNC/Phoenix.

Live-ID non-verified transactions are extremely useful to the Custody Officer as they are fast (typically received within 10 minutes of launch) and can be used 24 hours per day. They offer accuracy in excess of 98.5%. However, because they are automated and have not been looked at by expert FPOs, they should be treated as "intelligence" results only. Where any doubt exists in the mind of the Custody Officer following a Live-ID non verified result, then a verified Live-ID or a full Ten print Submission should be run in order to get a confirmed result from the Fingerprint Bureau.

Livescan retains and displays a single CRO that is returned as a result of a Non-verified Live-ID search response. The returned CRO is automatically input into the CRO field. The retained CRO appears when the user re-edits the form, and ensures that a retrieval search is initiated. This field may also be edited by the user if the user knows that the CRO returned by the non-verified search is correct.

Where any doubt exists in the mind of the Custody Officer following a Live-ID Non-verified result, then a full Ten Print Submission should be run in order to get a confirmed result from the Fingerprint Bureau.

Where an interface exists between a computerised custody system, such as NSPIS Custody, and Livescan, and a Live-ID search is requested from the custody system's screen, a result will also be passed back to the custody system.

3.2.3.4 **Print-to-Mark Crime Check**

The IDENT1 Livescan subsystem also provides the capability to perform a Print-to-Mark Crime Check. A Print-to-Mark search capability from Custody can be a very valuable tool since it can result in a PIC being identified for a previously unsolved crime before being released from the Custody office. A Print-to-Mark Crime Check may be requested through the Livescan HCI either at the same time the Live-ID Identity Check is requested, or separately. This allows for a Print-to-Mark search to be requested after the results of a Print-to-Print search have been received. If a transaction of the same type (i.e., Print-to-Print or Print-to-Mark) was previously submitted, the Livescan User will be presented with a warning, but will be permitted to over-ride the warning. The Print-to-Mark Crime Check is only available as a verified transaction.

A Print-to-Mark search launched as part of the Live-ID transaction becomes an AFR/Demographic search in IDENT1. While the default search is a local search and not filtered by crime type, the Livescan user has the option of modifying the Geographic Area and Crime Type selections. Geographic Area selections include the option for a national, regional, or local search, with the definition of regional being the default regional search specification of the local Bureau.

The search is carried out within IDENT1 as a new Print-to-Mark search thread, with a search priority set by the custody staff. A Print-to-Mark Crime Check requires all ten rolled impressions to be transmitted with the transaction. The same requirements that apply to a IDENT1 Print-to-Mark search apply to a Print-to-Mark submitted from a Livescan Workstation. These include three levels of comparison for an ident, notification of the owning bureau if an ident is made, etc. The response is returned directly to the Livescan workstation following the completion of the final comparison by the FPOs. A "Non-Ident" response simply indicates such, while an "Ident" response includes information to inform the

Livescan user that the PIC is identified for an offence, what offence, and when and where it took place. It may also be necessary in the case of an "Ident" for the Custody Staff to contact the Fingerprint Bureau by telephone to obtain additional details.

If the PIC is charged following the Live-ID search, the Livescan User may enter textual information into a "Notes" field on the Ten Print Submission HCI, such as whether a Print-to-Mark search was performed and its results. This information will be available to the FPOs during the processing of the Ten Print through the IDENT1 Bureau HCI and could be used to assist the IDENT1 Bureau staff in determining whether a P-M search is necessary as part of the Ten Print submission.

Where an interface exists between a computerised custody system, such as NSPIS Custody, and Livescan, and a P-M search is requested from the custody system's screen, a result is also be passed back to the custody system.

3.2.3.5 IND Search

A verified IND search can be initiated, intended to determine whether the identity of the PIC exists on the Immigration and Asylum Fingerprint System (IAFS). This option searches the IAFS system for the identity of the PIC. For an IND verified search request, two fingerprint officers check the search responses. AN IND non-verified search request searches the IAFS system for the PIC identity and returns a quick response for possible identification.

An additional benefit of searching IAFS is that the fingerprint records on the IAFS system may also hold a mug shot image of the PIC. If a search is successful on IAFS, and a mug shot image does exist for the PIC, then this image is contained with the respondent message at the Livescan station. This enables a second level of validation and identification at the Livescan unit. Up to five unique Immigration Fingerprint Bureau (IFB) Numbers, individual IND contact information, and any available photographs are displayed on the Livescan unit. A subsequent IND search using the returned IFB number retrieves the fingerprint record and any available photographs from the IAFS database.

Where an interface exists between a computerised custody system, such as NSPIS Custody, and Livescan, and an IND search is requested from the custody system's screen, a result is also be passed back to the custody system.

3.2.3.6 System Management

This section describes the functions considered to be "System Management" functions. Only a user designated as a IDENT1 Livescan Manager will be authorised to perform or access these functions.

- User Account Maintenance. (User Administration) User accounts with assigned User ID and Password combinations will be established by an authorised user (IDENT1 Livescan Manager) at each Custody Office. Each User ID/Password is valid at a specific IDENT1 Livescan workstation within a Custody Office, although nothing precludes the same User ID/Password being set for more than one workstation. A facility to allow a user to change his or her password is also provided through the HCI.
- Reports. The IDENT1 Management Information System (MIS) Tools function provides the capability to create ad hoc reports that can be used for tracking completed transactions, which were submitted via Livescan. Audit data is passed to IDENT1 as part of each transaction, and is recorded within the IDENT1 audit files. Additional audit data for user account maintenance, user logins and logouts, transmissions to and

from IDENT1, etc. are logged on the Livescan Workstation and requested by IDENT1 on a periodic basis.

3.2.4 User Level Threads

This section describes the various types of transactions supported by the IDENT1 Livescan subsystem, from the viewpoint of the Livescan user at the Custody Office.

3.2.4.1 Start-up/Shutdown

Upon powering on the Livescan workstation, the system boots and the required software processes are initiated automatically. The system then displays the Log-on screen and waits for the Livescan user to enter their User ID and password. This is recorded in the audit log.

The Livescan Workstation is connected automatically to the designated IDENT1 Bureau during the start-up process. If the connection to IDENT1 cannot be executed, the Livescan user is notified and has the option to operate the Livescan workstation in stand-alone mode.

Once the Livescan user has completed all tasks, he/she may choose to log-off or shut down the system from the Main Menu. After logging off, the Livescan user will have the option of shutting down the Livescan workstation. During shut down, all software processes are terminated and the Livescan user is instructed to power-off the Livescan workstation. Log-on, log-off, and shutdown activities are recorded in the audit log.

3.2.4.2 Logon/Logoff

Once the workstation is powered on, the Livescan user enters a User ID and the Livescan workstation main menu screen is displayed. In addition, each Livescan user is required to supply a valid User ID and Password combination to gain access to each of the Livescan Workstation applications. An authorised Livescan Manager will have assigned previously the User ID and Password and created the user account.

An audit trail log maintains the details of each transaction, to include information such as the initiating user, date and time, workstation ID, type of transaction, etc. In order to ensure that the user specified in the audit trail data is the actual user who initiated that transaction, the system prompts for the Livescan user's password to be entered before each Livescan or Live-ID transaction can be initiated. Upon completing his/her tasks, the Livescan user can choose to log-off from the Main Menu Screen.

3.2.4.3 Ten Print Capture

Ten Print capture begins by selecting the Livescan application. The Livescan user is prompted to enter a password for validation. A warning is displayed to the user if the available disk space has fallen below a specified threshold, and additional Livescan transactions are prevented from being initiated until disk space is freed up.

The initial step in the Livescan process is to create a Livescan transaction. This is done through selections made using the Livescan HCI, including the selection of the Ten Print Form Type. At this point, a unique Form Identification Number (FIN) will be assigned to the record.

The demographic and arrest data may be entered next. Alternatively, it is possible to enter the demographic data after the fingerprints have been captured. In practice, most users favour the latter option. Where an interface exists between an NSPIS Custody application (or

other computerised custody system) and IDENT1 Livescan, demographic information is passed automatically to Livescan and a Livescan record created and cued ready for fingerprints to be taken.

The next step is to capture the fingerprints. The Livescan User is prompted by the Livescan workstation HCI through each step of the capture process. First the plain impressions of right hand, left hand and both thumbs are taken, which enables an automatic sequence check to be performed as each finger is rolled.

Each rolled print is captured one at a time. As each rolled finger image is captured, the image is processed automatically for the purpose of determining its image quality and for comparison with the plain impressions. If the image falls below the system defined quality thresholds, the Livescan user is immediately notified of the reason. The Livescan user is prompted to capture the fingerprint again until either it is of acceptable quality or he or she over-rides the rejection. The HCI also enables recording of "Amputated" fingers or fingers "Not Taken" due to injury, which correspond to the standard IDENT1 fingerprint pattern classifications.

Once the rolled and plain impressions have been captured and processed, a verification match is attempted on the rolled impression and its corresponding plain impression. This is to perform an automated sequence check to determine if any fingers were rolled out of sequence. Any mismatches are reported immediately to the Livescan user, who must recapture the finger in question or over-ride the rejection. This eliminates the requirement for IDENT1 to perform a sequence check on Ten Print records submitted from an IDENT1 Livescan workstation.

Following capture of the rolled impressions, there is an opportunity for the user to review the fingerprints and retake any as necessary. Next the right and left palm prints are captured, including the "writer's edge", and the user again has the opportunity to review palm capture and retake if required.

There is also the capability to capture electronically the signature of the individual taking the prints, and that of the donor, via an integrated digital signature pad.

Next, the Livescan User has the option of submitting a Live-ID request or a Ten Print submission to IDENT1. Figure 3-3 shows the Ten Print Capture process.

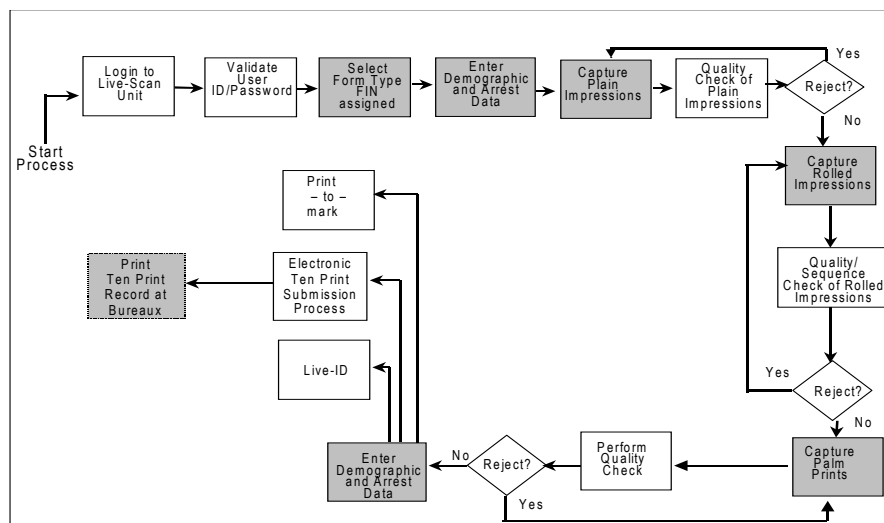


Figure 3-3 Ten Print Capture Process

3.2.4.4 Ten Print Submission

After entering the required demographic data and fingerprint images, and completing the quality checks, the Livescan user can choose to submit the ten print record to the designated IDENT1 bureau. Each of the fingerprint images (rolled and plain impressions) are compressed. A unique IDENT1 Form ID Number (FIN) was assigned previously to this Ten Print Record. Since any number of forms may be printed, with each being an exact reproduction of every other, every form contains the same FIN.

A unique transaction identifier is generated and assigned to the transaction. Finally, the record is formatted and sent to the designated IDENT1 bureau. The Arrest Summons (A/S) Number is required before a Ten Print Submission can be closed out on IDENT1, since it is required to communicate search results to PNC/Phoenix and for acquittal processing.

Whether the A/S Number is mandatory prior to Ten Print Submission, the Fingerprint Bureau is a configurable field. In practice, most police force users have set this field to be mandatory. Table 3-2 describes the data required for a Ten Print Livescan Submission. For an Arrestee form type, several of these fields are filled in automatically based on the Livescan workstation configuration data.

Table 3-2 Ten Print Livescan Submission Data Items

Data Item	Comments
Lossless Compressed Images (Rolled) Lossy Compressed Images (Plains and Palms)	10 rolled, 4 plain, and 4 palm images, sizes specified by IDENT1 image size requirements.
Form ID Number	Uniquely identifies the Ten Print Form.

CRO No.	This is optional, since CRO No. may not be known. IDENT1 will treat this as a Quoted CRO.
Arrest/Summons No.	Required by IDENT1 before the record can be closed out, but not required to be in the Ten Print Submission record.
Name, Sex, Charging Station, Owning Bureau, Taken By, Date Taken, DOB, Place of Offence, Crime Type	Required of all Ten Print Submissions to IDENT1
Alias/Maiden Name, Exhibit Identification number, Appearing/Cautioned, Court Name and Date, Nature of Disease, General Remarks, Notes	Optional

If the Ten Print record sent to IDENT1 is for submission only, the record is processed by IDENT1 as a standard Ten Print submission within the standard time frames allowed by the SLA. However, the Livescan User has the option of requesting Live-ID of the individual. The Live-ID transaction is described in Section 3.5.4.5.

3.2.4.5 Live-ID, Print-to-Mark, IND Search

After entering, or receiving, the required demographic data and taking the fingerprint images, the Livescan user can choose to request a search of the PIC using the captured fingerprint data. These search types are described in the following paragraphs. Table 3-4 describes the Data Items required for a Live-ID Identity Check request. The Livescan unit submits all ten fingers to perform the Live-ID search. A Print-to-Mark Crime Check contains all ten rolled impressions, does not contain CRO Number, and optionally contains geographic area designator and/or crime type. An IND search contains all ten rolled impressions, and optionally contains an Immigration Fingerprint Bureau (IFB) number.

Table 3-3 Live-ID Request Data Items

Data Item	Comments
Lossy Compressed Images (Rolled)	10 rolled, 35mm by 35mm.
Unique Transaction Identifier	Associated with IDENT1 Submission No.
CRO Number IFB Number (IND searches only)	This is optional, since CRO Number and IFB Number may not be known. If provided, a verification match will be performed by IDENT1.
Sex	Required for IDENT1 P-P Search, can be unknown

Where an interface exists between a computerised custody system, such as NSPIS Custody, and Livescan, and a search is requested from the custody system's screen, a result is also passed back to the custody system.

Verified Response

The Livescan user can request that a search be verified by an FPO. The “verified response” function allows the Livescan User to select Live-ID Identity Check, Print-to-Mark Crime Check.

The Livescan user initiates a transaction by entering the “suggested” or “quoted” CRO Number of the PIC (if known) and the sex of the PIC, then makes a search type selection through the HCI.

Each of the fingerprint images must be compressed and transmitted with the transaction. The images and required demographic data are packaged as a CPS Message with the appropriate transaction type. The search request is sent to the IDENT1 bureau designated for that Custody Office.

If a match is found, the respondent images are queued for FPO verification. Two FPOs verify the results of the IDENT1 AFR search by viewing the images. A “No Match” or “Verified Match” with the individual’s CRO Number is sent back to the Livescan Workstation. The response also includes an indication that the search results have been verified.

The Print-to-Mark Crime check is a verified search request. The P-M Crime Check search request provides options for the Livescan user to change the defaults for the Crime Type and Geographic Area. The Livescan user may select a local, regional, or national search. Overriding the default search results in a confirmation warning being displayed to the Livescan user. The P-M search request requires all ten rolled impressions to be submitted with the transaction.

The Livescan user can also request a verified IND search. The IND search option allows the Livescan user to input an Immigration Fingerprint Bureau (IFB) number to the search request. The IFB number performs a retrieval from IAFS rather than a full search against the IND database. The quoted IFB number works in the same way as a quoted CRO against IDENT1. If available, IAFS returns an accompanying mug shot photograph to the Livescan unit for display along with the respondent data.

If a match is found, the results are queued for FPO verification viewing. The images are verified by three FPOs prior to returning a response to the Livescan workstation. A “Non Ident” or “Verified Ident” will be sent back to the Livescan workstation. The “Verified Ident” response will contain sufficient information to inform the Livescan user that the PIC is identified for an offence, what the offence type is, and when and where it took place. It may also be necessary in the case of an “Ident” for the Custody Staff to contact the Fingerprint Bureau by telephone to obtain additional details.

The Livescan user may request a P-M search after results from the live-ID search have been received. If a search of the same type was submitted previously, the Livescan user is presented with a warning; the warning can be overridden.

If the PIC is charged following the search, the Livescan user may enter textual information into a “Notes” field on the Ten Print Submission HCI, e.g., whether a P-M search was performed and its results. This information will be available to the FPOs during the processing of the Ten Print submission at the Bureau through the “Notes” function.

Non-Verified Response

The Livescan user can also request a fully automated search and result; a non-verified Live-ID response. Non-verified Live-ID requests cannot include a CRO number. In this instance, only an AFR comparison is performed. The search results are then sent directly to the Livescan workstation, and include a CRO Number and Match Confidence for each respondent with a score above the Live-ID match threshold. The response will clearly indicate that the results have not been verified by FPOs. Livescan functionality will retain and display the single, high confidence CRO that is returned as a result of a Live-ID non-verified search responses. The CRO will automatically be input into the CRO field. The retained CRO will appear when the user re-edits the form, and ensures that a retrieval search is initiated on Ten Print Submission. This field may also be edited by the user if the user knows that the returned CRO is correct.

The Livescan user can also request a non-verified IND search. Non-verified IND requests may include an IFB number.

3.2.4.6 Delete Transaction

Ten Print records are stored within the Livescan workstation until the Livescan user specifically deletes the transaction, or the system automatically deletes them following the successful closeout of the transaction on IDENT1. The usual reason for the record to be deleted manually is in the case of wrongful arrest or if it is decided that there will be no further action (NFA). The deletion of the form following closeout results from the auto delay value. This configuration parameter is set on each Livescan unit.

3.2.4.7 Local/Remote Printing

The Livescan workstation architecture supports local and remote printing of Livescan ten print records, although in practice the option to have a local printer alongside the Livescan unit has not been taken up by the users and the Livescan printer is sited remotely at the local Fingerprint Bureau.

Since a hard copy ten print form is required for IDENT1 "Close-Out" of a ten print submission, the form must be printed out prior to Close-out. The printing of a ten print form occurs when the ten print submission is first processed on the store and forward unit, and prior to IDENT1 processing.

3.2.4.8 System Management

The System Management functions require that a user login using a user ID and password combination with System Manager privileges. Menu selections provide access to the following System Management functions:

- Configuring the system, which includes:
 - Setting the system time and date
 - Maintaining the user list
 - Saving the system configuration
 - Reloading the system configuration

- Reports
- Adjusting the Printer

The system date and time used internally by the Livescan workstation will be set during the initial installation and setup of the unit. The system date and time is used for logging and time stamping of transactions.

User Accounts are created, deleted, modified, or viewed through the User Account Management function. The user's full name, printed name (as it appears on fingerprint forms), user ID, user password, and authorisation level (manager or user) is entered to create an account. Each Livescan workstation maintains its own list of authorised users.

A Livescan workstation's configuration data can be saved to a file, which allows either the same workstation or another workstation to be restored with that data. The configuration data includes the user account information, printer settings, calibration data, fingerprint form options, demographic defaults, IP addresses, etc.

Each Livescan workstation collects audit data in two modes. First, data specific to a transaction is transmitted to the IDENT1 bureau with each transaction. Second, audit data for user account maintenance, user logins and logouts, fingerprint capture sessions, record deletion, and IDENT1 transmissions is transmitted to the IDENT1 bureau upon request. This permits the IDENT1 bureau and central segments to produce reports that include Livescan information.

The Livescan printer can be adjusted periodically to adjust the range of print darkness (ramping) or position of fingerprints and demographics on a printed ten pPrint form. This procedure is recommended whenever a new toner cartridge is installed or degradation is noticed in the darkness of the printed fingerprint images.

3.2.5 System Maintenance

This section describes the maintenance for the Livescan workstation. System maintenance for the Livescan workstation includes four levels of support:

- First Level - Replacement of consumables and cleaning of units
- Second Level - Replacement of Line Replaceable Units (LRUs)
- Third Level - Servicing of equipment off-site
- Fourth Level - Design/development changes.

The first level maintenance is the responsibility of the authorised and trained Livescan users and includes cleaning of the platen(s), cleaning/replacing air filters, replacing printer toner, and replenishing the fingerprint form stock in the printers.

The second level maintenance is performed by the IDENT1 Northrop Grumman maintenance team as part of the regular inspections of the equipment or in response to service calls logged through the IDENT1 help desk. Spares stocks are maintained by Northrop Grumman and used to repair and re-calibrate the equipment. On-line diagnostics are available for troubleshooting the equipment, and each removed LRU is designated as either scrap or depot repairable.

The third level of service is performed at either the manufacturer's facility (e.g., unique equipment such as the optical decks) or at the Northrop Grumman maintenance facility (for those components that are evaluated readily and for which standard components are available

(e. g., computer components, Ethernet cards, etc.). These repaired components are re-certified and returned to the spares stocks when repairs are completed.

The fourth level of service is for system improvements for which a business case can be presented and substantiated. These may be based upon user demands or due to the introduction of new technologies. Those that are approved are scheduled for implementation and fielding according to the perceived benefits, costs, and update schedules.

3.2.5.1 Help Desk

The IDENT1 Help Desk is responsible for overall maintenance support. The Help Desk will be staffed 24 hours-a-day, 365 days a year to provide initial response to any local Police Force's operational problem with either the equipment or communications, including any interface problems. The Help Desk is accessed via telephone for direct conversations with a Help Desk technician. The Help Desk provides first level diagnostic evaluation of the problem, including remote diagnostic execution, examination of audit records, and general recovery techniques (e.g., recycling power, etc.). Problems that cannot be resolved by the Help Desk personnel are assigned to field maintenance personnel for repair.

Any requests for operational support received by the Help Desk are logged automatically in a trouble call tracking system. Through management information maintained in the maintenance tracking system, the Help Desk user is able to assess the impact of the incident (degradation of operations versus complete loss of functionality) to quickly and accurately take appropriate action. The Help Desk technicians have remote login capabilities to each Livescan workstation. In order to maintain system security/integrity, the remote login capability is only be available from the Help Desk and is only available to authorised personnel. The Help Desk personnel may request additional diagnostic information from the on-site personnel, or may request they attempt to correct/eliminate the problem (for example, re-boot a workstation, check a LAN connection, etc.).

The Help Desk also provides management reports and metrics on outstanding incidents, major incidents, and maintenance trends (problem hardware items, Help Desk call frequency, repeat discrepancies). However, if remote actions are not effective in correcting the problem, escalation procedures are initiated to provide on-site maintenance resources.

3.2.5.2 On-Site Support

On-site support is provided for the operational Livescan workstation whenever Help Desk support or first line maintenance is insufficient in bringing the equipment back to full operational capability. The Help Desk initiates escalation procedures to issue a work request for the maintenance technicians. The work request includes the initial information contained in the trouble call: the location of the equipment, point of contact, maintenance problem, time of call, data collected and actions taken, and any site specific information.

Any equipment items, which are replaced for maintenance purposes, are returned to a Northrop Grumman repair location for third level maintenance actions. Maintenance at the third level includes a repair analysis to determine if the item is repairable economically, or whether replacement is appropriate.

Regardless of the disposition, Northrop Grumman monitors the maintenance turnaround time at the third level to ensure that the Livescan workstation stock of spares is adequate to meet operational commitments.

4 REQUIREMENTS

This section details the IDENT1 Livescan subsystem (ILSS) requirements which are grouped into the following subsections: General Requirements, Functional Requirements, Configuration Parameters, System Performance, System Management, Security, and IDENT1 Modifications requirements. Cardinal requirements are high level and avoid implementation constraints where possible. They are wide ranging in scope and cannot be implemented directly but require decomposition. The cardinal requirements are numbered with a prefix "CC," while all other requirements are prefixed "CL" and are detailed requirements derived from the cardinal requirements. The majority of "CC" requirements are in section 4.1, General Requirements; while some others have been allocated to specific sections.

4.1 General Requirements

The requirements in this section are cardinal requirements that apply to the entire ILSS and not a specific function or component.

- | | |
|-------|--|
| CC001 | Northrop Grumman shall investigate, determine the requirements, develop, implement and supply remote fingerprint services integrated with the operational procedures at designated charging stations as a complete and integrated extension of the IDENT1 system. These are in any combination: (a) Remote electronic Ten Print capture and submission services. (b) Remote Palm Print services (optional). (c) Remote Live-ID services. |
| CC002 | The ILSS as defined in this specification shall be subject to Service Level Requirements (SLR). The core remote service may be augmented with additional remote services, each additional service shall meet the general, core and specific service requirements and the core remote service SLR shall be extended to incorporate service performance for all additional remote services. |
| CC003 | Northrop Grumman shall provide prime contractor and IDENT1 system integration services and shall be fully accountable for the technical delivery of the ILSS. This shall include all consequential impacts required to meet and sustain the service level of IDENT1. |
| CC004 | The performance, service levels, metrics, workload, credit/debit and response times, of the ILSS shall be defined in a SLR. |
| CC005 | The ILSS shall obtain fingerprint data from a Livescan workstation provided with optional palm print capabilities. |
| CC006 | No specialist skills shall be required by the ILSS users other than those required for operational employment of the ILSS (e.g., engineering skills for calibration, management or servicing shall not be required of the charging users). |
| CC007 | Provisions for training of ILSS users and bureau staff shall be determined and provided. |
| CC008 | Acceptable fallback procedures shall be provided if the ILSS unit is taken out of service, or must operate in isolation. |

- CC009 The ILSS shall be appropriately integrated into the support and maintenance of the IDENT1 system.
- CC010 ILSS Live-ID transactions shall be delivered to a primary local bureau or to an alternative bureau selected by the local bureau and agreed by Northrop Grumman. Services shall continue to be available at the Livescan workstation when the primary bureaux is completely unmanned.
- CC011 ILSS capture devices shall conform to the FBI, Criminal Justice Information Services (CJIS) Electronic Fingerprint Transmission Specification (EFTS) standards, FBI CJIS-RS-010 V7 (January 1999) "Image Quality Specifications (IQS)", Appendix F.
- CC012 The ILSS shall comply with all relevant UK legislation that is in effect at the time approved for entry into the IDENT1 catalogue of options.
- CC013 The ILSS shall comply with relevant health and safety requirements at the time approved for entry into the IDENT1 catalogue of options.
- CC026 The ILSS vendor shall provide fully configured Livescan units with all processing components necessary (e.g., processors, monitors, disks, etc) and hardware (e.g., case, cables, etc.) to capture and transmit electronic ten print records to remote sites for printing and forward to IDENT1.

4.2 Functional Requirements

Functional requirements are divided into three distinct categories: Electronic Ten Print Capture, Electronic Ten Print Submission, and Live-ID.

4.2.1 Ten Print Capture

The ILSS includes the capability to perform ten print capture, which provides a means of electronically capturing all rolled impressions, plain impressions, and palm prints directly from an individual's hand without the use of ink. Also, included in the capture process is the entry of demographic and arrest data; and automated quality checks.

The quality checks, to include image quality, sequence check, and demographic data validation are performed as part of this process. The image quality check ensures that the fingerprint images are acceptable for processing by IDENT1. The sequence check ensures that the rolled fingerprints were captured in the proper order. Once the images and the demographic data are successfully captured and accepted, the Livescan user has the capability to print the ten print form provided the optional local printer has been included.

- CL001 The Livescan workstation shall provide a means of electronically capturing plain finger impressions, all ten rolled finger impressions, and palm impressions (optional) including the writer's edge directly from an individual's hands without the use of ink.
- CL002 The ordering and content of the demographic data presented on the IDENT1 Livescan HCI shall be based on the IDENT1 ten print forms.
- CL003 The Livescan workstation shall allow the user to enter demographic and arrest data to be included with the electronic ten print submission as specified by the Livescan-IDENT1 Interface Specification.

- CL004 The Livescan workstation shall conform with FBI Standard CJIS-RS-0010(V7) "Interim IAFIS Image Quality Specifications for Scanners", Appendix G, for image capture, plus all non-conflicting requirements given in the full Image Quality Specification (IQS), Appendix F.
- CL005 The sizes of the fingerprint images captured by the Livescan workstation shall be consistent with the IDENT1 image sizes. These are 689 by 689 pixels for rolled impressions, 749 by 452 pixels for plain thumb impressions, and 1477 by 1182 pixels for plain finger impressions, all captured at 500 dpi.
- CL006 The fingerprint image quality shall be assessed in real time to produce immediate quality feedback to the Livescan uUser.
- CL007 The Livescan workstation quality control software shall have the facility of allowing the Livescan user to over-ride an image quality rejection.
- CL008 When the quality of an image is below the quality threshold setting(s), the Livescan user shall be prompted to perform corrective action to include recapturing the print image.
- CL009 The Livescan workstation shall record, for each transaction, whenever the Livescan user chooses to over-ride the system quality rejection.
- CL010 The Livescan workstation shall perform an automated sequence check that verifies the correct sequence of the rolled impressions as compared to the plain impressions.
- CL011 When the automatic sequence check process is unable to match a rolled and plain impression, the Livescan user shall be notified immediately and given an option to recapture the images.
- CL012 The Livescan workstation shall be capable of capturing new fingerprint records whilst transactions are being transmitted.
- CL013 The Livescan workstation HCI shall allow the Livescan user to specify that a finger is "Amputated" or "Not Taken" due to injury.
- CL014 A finger specified as "Amputated" or "Not Taken" shall be recorded in the ten print record, indicated on the screen, and on the ten print form within the appropriate fingerprint boxes.
- CL015 The Livescan workstation HCI shall support each of the standard IDENT1 ten print form types.
- CL016 The Livescan workstation HCI shall have required data fields that are specific for each IDENT1 ten print form type and transaction type (e.g., Live-ID or ETPS). The required fields are specified in the Livescan IDENT1 Interface Specification.
- CL017 The Livescan workstation HCI shall indicate the current forms type during the capture processing.
- CL018 The Livescan workstation shall be able to capture, print locally (optional), and submit Ten Print records to IDENT1 for the following ten print form

- types: Arrestee, Suspect Not Charged, Caution, Prison, Amnesiac, and Elimination.
- CL019 Elimination sets shall be printed on the IDENT1 Elimination form and all other sets shall be printed on the IDENT1 Arrestee form.
- CL020 Elimination sets shall not be processed by IDENT1.
- CL021 Additional Livescan transactions shall be prevented from being initiated if sufficient space is not available.
- CL022 Previously captured ten print records on the Livescan workstation shall not be lost if the disk space is full, unless explicitly deleted by the Livescan user.
- CL023 The Livescan workstation shall provide the capability option to print a ten print locally.
- CL024 Any optional Livescan printer used with the Livescan workstation shall conform to FBI Standard CJIS-RS-0010(V7) Appendix F, "Printer Specifications".
- CL025 Livescan printers shall be able to print multiple copies of ten print forms.
- CL026 The Livescan workstation shall generate a Form ID No. for each ten print record once the record has been accepted by the Livescan uUser.
- CL027 The format of the Form ID No. generated by the Livescan workstation shall be as follows: AA/BB/CC/DDDDDDDD/E, where AA is a two character Form Type, defined with the following codes:
- "LA" for Livescan Arrestee Form,
 - "LS" for Livescan Suspect Form,
 - "LE" for Livescan Elimination Form,
 - "LP" for Livescan Prison Form,
 - "LO" for Livescan Other Form,
 - "LN" for Livescan Amnesiac Form;
 - BB is a two character Form Format, defined with the following codes:
 - "NA" for a standard Livescan form format;
 - CC is a two character predefined Livescan workstation designator, allowing 1296 unique Livescan designations for the UK Police Forces;
 - DDDDDDD is a seven digit sequential number unique for a single Livescan workstation;
 - and E is the check character generated using the standard Phoenix modulus 23 algorithm.
- CL028 The equipment shall conform to the following safety standards: 73/23/EEC (1973) Low Voltage Directive with Amendments; UL 1950 (1995) Third Edition; Bi-National Safety of Information Technology Equipment including Electrical Business Equipment; IEC 950 (1991) (EN60950) Safety of

Information Technology Equipment, including Electrical Business Equipment, Electromagnetic Compatibility, FCC Rules Part 15 for Class A Computing Devices; 89/336/EEC (1989) EMC Directive; EN55022 (1995) Limits & Methods of Measurement of Radio Interference; Information Technology Equipment; and EN50082 Electromagnetic Compatibility Generic Immunity Standard.

- CL029 The Livescan HCI shall provide a capability to delete a ten print record from the Livescan workstation.
- CL030 The Livescan HCI shall warn a Livescan user if a user attempts to delete a ten print record from the Livescan workstation before the record is successfully received by the IDENT1 bureau.
- CL114 The Livescan user shall be given an indication as to the available disk space or number of available transactions on the Livescan workstation.
- CL115 The Livescan images printed onto a Ten Print Form shall be printed using the full capture size and resolution specified for the Livescan workstation, i.e., captured image to print ratio of 1:1.
- CL116 The Livescan workstation shall optionally provide a capability to electronically capture and transmit the identity of the individual taking the prints (e.g., electronic image of signature or fingerprint).
- CL117 The Livescan workstation shall optionally provide a capability to electronically capture the signature image of the PIC.
- CL118 The INLSS shall support the local printing of IDENT1 fingerprint forms on pre-printed IDENT1 forms.
- CC014 The Livescan workstation shall capture all fingerprints and palms (optional) concerning one person in custody in one fingerprinting session.
- CC015 Once the fingerprint data is captured at the Livescan workstation it shall then be used as a source for all transactions until deleted by the Livescan user.
- CC016 Responses to search requests with identification shall be returned to the submitting Livescan workstation.
- CC017 Optional palm prints shall be electronically captured by the ILSS.
- CC018 Optional palm prints shall be captured, transferred to the bureau, and printed out on the fingerprint form such that they may be utilised subsequently for evidence and matching purposes.

4.2.2 Ten Print Submission

The INLSS includes the capability to electronically transmit ten print submissions to IDENT1. Through the electronic ten print submission process, the Livescan user submits a ten print record to the designated IDENT1 bureau. Each of the fingerprint images (rolled and plain impressions) is compressed, a unique transaction identifier is generated and assigned to the transaction, and the record is formatted and sent to the designated IDENT1 bureau.

- CL031 The Electronic Ten Print Submission record shall include up to ten rolled finger impressions (lossless); four plain impressions (lossy); two (optional) palm prints (lossy); two (optional) writer's edge (lossy); required demographic and arrest data; and audit data. The format in content of the record is specified in the Livescan IDENT1 Interface Specification.
- CL032 All fingerprint data transmitted electronically to the designated IDENT1 Fingerprint Bureau shall be compressed and decompressed using the same JPEG algorithms used by IDENT1.
- CL033 Every electronic ten print record submitted to IDENT1 by the Livescan Workstation shall include appropriate audit data (e.g., Livescan User ID, transaction type, unique ID, date and time of submission, Livescan workstation ID, quality override data, and destination ID)
- CL034 The ILSS shall print a ten print form remotely at the designated IDENT1 bureau.
- CL143 The remote printer shall conform to FBI Standard CJIS-RS-0010(V7) "Printer Specifications", Appendix F.
- CL036 A Form ID number shall be assigned by the Livescan workstation and stored with the electronic ten print submission.
- CL037 A Form ID No. shall be printed on the ten print form in both bar-code and human readable form.
- CL038 The Form ID No. bar-code format shall comply with the following specifications; ANSI MH10.8M-1993, American National Standard for Materials Handling - Unit Loads and Transport Packages - Bar Code Symbols and AIM Uniform Symbology Specification Code 39.
- CL039 The response displayed to a user at the Livescan workstation for an electronic ten print submission ident response shall include a CRO Number. For a Non-Ident response only the Non-Ident status is displayed.
- CL040 The Livescan workstation shall receive a response message from the IDENT1 bureau indicating that the initial ten print submission was received and validated by IDENT1. The format in content of this message is specified in the Livescan IDENT1 Interface Specification.
- CL041 The Livescan workstation shall receive a message from IDENT1 once the final level of P-P comparison is made for an Ident and following a CRO assignment for a Non-Ident by IDENT1. The format in content of this message is specified in the Livescan-IDENT1 Interface Specification.
- CL042 The Livescan workstation shall receive an error message from IDENT1 if an error is detected during the processing of a ten print submission record. The format in content of this message is specified in the Livescan IDENT1 Interface Specification.
- CL043 All response messages sent to an unavailable (e.g., powered down, communication down) Livescan workstation shall not be lost and will be transmitted once the Livescan workstation is available.

- CL044 All response messages received from IDENT1 by the Livescan workstation shall be available for display to the Livescan user.
- CL045 All electronic Ten Print submissions generated by the ILSS shall be assigned the search priority selected by the Livescan user.
- CL159 Livescan search priority shall be configured to “normal” for all searches.
- CL119 An indication shall be displayed to the Livescan user if a ten print submission transaction is requested for the same ten print record more than once.
- CL120 The images and data from an electronic ten print submission shall be capable of being stored and retrieved from the Bureau Image Archive.
- CL121 The optional palm print images shall be included in the electronic submission to IDENT1.
- CL122 The store and forward device shall have the capacity to queue a minimum of 250 transactions.
- CL123 The ILSS shall support the entry of free text notes entered through the Livescan workstation HCI and submitted with the electronic ten print submission transaction to the IDENT1 bureau for inclusion into the IDENT1 ten print mManagement notes function.

4.2.3 Live-ID Identity Check, Print-to-Mark Crime Check, IND Search

The ILSS includes the capability to perform a Live-ID Identity Check of a person in custody for the purpose of providing a quick identification. Live-ID is a non-verified ten finger Print-to-Print search against the IDENT1 ten print database, or a one-to-one verification if a CRO number is provided. For an IND Search, a one-to-one verification is activated if an IFB number is provided. The Livescan user also has the option of selecting either a verified or a non-verified response. Print-to-Mark Crime Check searches are always verified. A verified response includes a fingerprint comparison by two FPOs. A non-verified response only consists of an AFR P-P comparison without the involvement of a FPO, with the results sent directly to the submitting Livescan workstation.

- CL046 The ILSS Live-ID Identity Check function shall support a ten-finger Print-to-Print search.
- CL047 The fingerprint images for all Live-ID transaction shall be chosen from the ten print record captured during the Livescan electronic ten print capture process.
- CL124 REQUIREMENT DELETED
- CL136 A Print-to-Mark Crime Check search shall use the rolled impressions of all available fingers.
- CL048 A minimum of one finger shall be required to initiate a Live-ID transaction.
- CL049 The Livescan user shall select either a verified or non-verified response from the Livescan workstation HCI for each Live-ID Identity Check transaction.

- CL050 The Livescan workstation shall provide the capability for a user to submit a quoted CRO for verified Live-ID transactions, resulting in a one-to-one verification performed at the IDENT1 bureau.
- CL051 The Livescan workstation HCI shall require only those data entry fields needed for a Live-ID transaction to be entered before a Live-ID transaction can be submitted.
- CL052 The Livescan workstation shall be able to submit a Live-ID transaction while retaining the ten print data at the Livescan workstation.
- CL053 The Live-ID function shall result in IDENT1 initiating a default Print-to-Print AFR search if a non-verified response was requested.
- CL054 The Live-ID function shall result in IDENT1 initiating a Print-to-Print one-to-one verification (i.e., FPO comparison of the images) if a verified response was requested.
- CL055 The Live-ID HCI shall permit a CRO Number to be entered when a non-verified Live-ID transaction is being requested.
- CL149 Livescan shall retain a quoted CRO. The retained CRO will appear when the user re-edits the form, and ensures that a retrieval search is initiated.
- CL150 For non-verified quoted CRO Live-ID respondents, the retained quoted CRO is electronically compared against the respondent CROs. Each CRO number shall include a match/mismatch display for the Livescan user.
- CL056 If a Live-ID one-to-one verification from a verified quoted CRO Number results in a non-ident, then IDENT1 shall automatically perform a print-to-print AFR search.
- CL057 The response displayed to a user at the Livescan Workstation for a Live-ID non-verified response shall include zero or more respondent(s) and a disclaimer stating that the search has not been verified by a qualified Fingerprint Officer. For each respondent a CRO number and match confidence shall be displayed.
- CL058 The response displayed to a user at the Livescan workstation for a Live-ID verified response shall include a CRO Number for an Identification or a Non-Ident status.
- CL059 The Livescan workstation shall receive a response message from the IDENT1 bureau indicating that the initial Live-ID transaction was received and validated by IDENT1. The format and content of this message is specified in the Livescan IDENT1 Interface Specification.
- CL060 The Livescan workstation shall receive a message from IDENT1 once the Live-ID transaction has been completed by IDENT1. Two levels of comparison check shall be required prior to a verified Print-to-Print response being sent to the Livescan workstation. The format and content of this message is specified in the Livescan IDENT1 Interface Specification.

CL061	The Livescan workstation shall receive an error message from IDENT1 if an error is detected during the processing of Live-ID transaction. The format and content of this message is specified in the Livescan IDENT1 Interface Specification.
CL062	All Live-ID response messages sent to an unavailable (e.g., powered down, communication down) Livescan workstation shall not be lost and will be transmitted once the Livescan workstation is available.
CL063	All Live-ID response messages received from IDENT1 by the Livescan workstation shall be available for display to the Livescan user.
CL064	All Live-ID transactions generated by the ILSS shall be assigned the search priority selected by the Livescan user.
CL125	The ILSS shall support a Print-to-Mark search through the HCI.
CL126	The Print-to-Mark Crime Check search shall only be requested in conjunction with a “verified response.”
CL127	The Livescan workstation HCI shall support the selection of a Print-to-Mark Search either combined with a Live-ID search or independently.
CL128	All Print-to-Mark searches initiated from the ILSS shall be assigned the search priority selected by the Livescan user.
CL159	Livescan search priority shall be configured to “normal” for all searches.
CL129	An indication shall be presented to the Livescan user whenever a Live-ID search of the same type (e.g., Live-ID or Print-to-Mark or IND) is initiated for the same ten pPrint record.
CL130	All Print-to-Mark searches shall be implemented within IDENT1 as a default Print-to-Mark AFR search, unless a Crime Type or non-default Geographic Area is specified.
CL131	The ILSS HCI shall allow the Livescan user to select a geographical region for Print-to-Mark searches.
CL132	For all Print-to-Mark searches with a Geographic Area set to “Regional”, the default search specification of the local bureau shall be used for the Region definition.
CL133	A separate response message shall be returned to the Livescan workstation for the Print-Mark search and shall include sufficient information to convey to the Livescan user that the PIC may be a suspect in other crimes and the Livescan user should contact the bureau.
CL134	REQUIREMENT DELETED
CL135	P-M searches shall require three levels of FPO comparison prior to returning a verified match response to the Livescan user.
CC019	No additions, modifications or deletion of information held in national or local fingerprint collections shall occur as a result of a Live-ID transaction.

- CL151 The IND Search function shall request an IAFS Print-to-Print search against the Immigration and Naturalisation Database.
- CL152 For an IND Search with a quoted IFB Number, Livescan shall request retrieval of the IND images associated with the IFB form identification number.
- CL153 For an IND Search, an available IAFS mug shot image shall be returned to Livescan with the IFB number. There will be a maximum of one image for each respondent in the respondent message.
- CL154 For non-verified quoted IFB IND respondents, the retained quoted IFB number is electronically compared against the respondent IFBs. Each IFB number shall include a match/mismatch display for the Livescan user.
- CL155 A separate response message shall be returned to the Livescan workstation for the IND search and shall include sufficient information to convey to the Livescan user that the PIC may be a suspect in other crimes.

4.3 Configuration Parameters

The Livescan workstation has various parameters that are configurable by the Service Provider. Configuration parameters provide a means of changing configuration options without the need for software modifications, thus increasing the flexibility and maintainability of the system. Modification privileges will be assigned according to the function performed by each parameter.

- CL065 The image quality threshold for images captured at the Livescan workstation shall be configurable by the service provider and not accessible by Users.
- CL066 The number of times the Livescan user must re-scan an image that fails the image quality checks before overriding the "image quality failure" warning shall be configurable by the service provider.
- CL067 The ILSS shall have the capability for the form layout to be modified by the service provider.
- CL068 Configuration parameters set only by the service provider shall specify which NLSS options (e.g., palm capture, local printer) are installed.
- CL069 A configuration parameter shall specify the number of ten print forms printed by the Livescan Store and Forward at the bureau.
- CL070 A configuration parameter set only by the service provider shall specify which is the active IDENT1 bureau for a specific Live Scan workstation.
- CL071 A configuration parameter shall specify the screen lock inactivity period and will be set by the service provider.
- CL137 REQUIREMENT DELETED

4.4 System Performance

The System Performance requirements state the capacity, quality, timeliness and availability of the ILSS.

CC020	It shall be possible for a trained user to complete the electronic ten print capture process within 15 minutes using a Livescan workstation. This includes required demographic data entry, image capture including optional palms, all quality checks, and saving data locally.
CC021	The transfer of the data for electronic ten print submission and Live-ID transaction shall occur in a timely manner without any additional effort at the custody office station or fingerprint bureau.
CC022	The ILSS will be available 24hrs a day 7 days a week on demand from the charging station users. Operational availability shall be determined for each unit at the charging station as described in the IDENT1 Livescan Service Level Requirements.
CC023	The quality and integrity of all data captured, processed, and stored by the ILSS shall not be degraded by the use of capture devices integrated into the extended system.
CL072	REQUIREMENT DELETED
CL073	REQUIREMENT DELETED
CL074	REQUIREMENT DELETED
CL075	REQUIREMENT DELETED
CL076	REQUIREMENT DELETED
CL077	The Livescan workstation shall be capable of storing a minimum of 250 Livescan transactions.
CL138	REQUIREMENT DELETED
CL139	REQUIREMENT DELETED
CL146	REQUIREMENT DELETED

4.5 System Management

The System Management functions for the IDENT1 Livescan subsystem (ILSS) are available to all users with Livescan Manager authorisation. Access privileges are established by each Custody Office and assigned to each user's account at the time of creation; the privileges can also be modified at any time by a user with the proper authorisation. The System Management functions are accessed from the Livescan workstation main menu. Two levels of system management functions are available for the IDENT1 Livescan subsystem: Reporting and management functions, and system administration functions.

4.5.1 Reporting and Management

Reporting and management functions are performed by users with Livescan Manager authorisation. These include the capability of generating standardised reports (e.g., event summary logs, and statistical summaries); and user account management to create user accounts and assign access privileges.

- CL078 The ILSS shall provide the capability for an authorised user to create IDENT1 Livescan User accounts for a specific ILSS workstation. Create and delete a user account includes specifying a User ID, default password, and the User's actual name.
- CL079 REQUIREMENT DELETED
- CL080 A Livescan Manager shall have the capability to view or modify those Configuration Parameters for which he/she is authorised.

4.5.2 System Administration

System administration functions are performed by Northrop Grumman support personnel. These functions are performed locally or remotely from the Central Site. They include Operating System Maintenance; Scanner Calibration; System Configuration Parameters; Application Software Management; and System Monitoring.

- CL081 The ILSS workstation shall provide sufficient software utilities to support the maintenance of the workstation's operating system.
- CL082 A capability shall be provided to check the calibration, if necessary, of ILSS fingerprint capture devices.
- CL083 An authorised user shall have the capability to view or modify any ILSS Configuration Parameters including those designated for Service Provider.
- CL084 A capability to update electronically the software on a particular ILSS Workstation from the IDENT1 central segment shall be provided.

4.6 Security

Security includes integrity, confidentiality, and availability of the information held and processed by the ILSS. Security requirements are decomposed into five categories: Facility, Identification and Authentication, Access Control, Audit, and External/Internal Interface requirements. The Livescan workstation resides within a Custody Office, which is a physically secured environment. Therefore, the Facility requirements are not included in this specification.

4.6.1 Identification and Authentication Requirements

Identification is a statement of who the ILSS user is. The process of verifying a user's claimed identity is authentication. ILSS users must identify themselves to the ILSS and the system must verify their identity. The user's authenticated identity is used to control access to the ILSS and provide accountability with respect the user's actions while using the ILSS.

- CL085 Each user shall be assigned a unique User ID and Password combination to be used for purposes of limiting access to ILSS functions and for tracking transactions by user.
- CL086 Initially, passwords shall be assigned by a Livescan Manager and changed by the Livescan user thereafter.

- CL087 The passwords shall be stored in encrypted form. Passwords will always be transmitted in the encrypted form. The plain version of password will not be stored in the system.
- CL088 Passwords shall not be displayed on screen. For example, an asterisk may be echoed to the screen as each character of the password is typed.
- CL089 A Change Password facility shall be provided in the ILSS to allow an authorised user to change his or her password after entry of the original password.
- CL090 The ILSS shall support the capability to set passwords to expire after a specified period of time.
- CL091 The ILSS shall prevent modification of the fingerprint image portion of the Livescan ten pPrint record once the capture process has been completed and accepted by the operator.
- CL092 The Livescan workstation shall lock the screen after a specified inactivity period and provide the capability to unlock the screen.

4.6.2 Access Control Requirements

Access controls restrict access to objects based on the identity of the user and the authorisations assigned to that user. Objects receive or contain information, e.g., records, directories, directory trees, files, and programs, workstations, servers, etc.

- CL093 Access to the system shall be restricted. This may be achieved though the use of physical security measures, personal identification schemes or a combination of the two.
- CL147 Each Livescan transaction shall require a separate login.
- CL148 The ILSS shall automatically logout a user upon completion of a Livescan transaction.
- CL094 Each authorised Livescan user shall be assigned a specific role corresponding to their User ID and password, that will limit their access to the Livescan Workstation to specific permitted functions.
- CL095 The ILSS shall support at least three roles; Livescan User, Livescan Manager, and System Administrator. Only the service provider maintenance staff will be authorised as a System Administrator role.
- CL149 A System Administrator or Livescan Manager shall not be able to amend their own Livescan transaction records in any way, through their own or different accounts.
- CL150 A System Administrator or Livescan Manager shall not have Livescan user privileges and vice versa.
- CL096 A shutdown mechanism shall be provided for use by the Livescan manager.
- CL097 Following logout the screen shall be cleared and a new login screen displayed.

4.6.3 Audit Requirements

Definition of audit requirements enables activities on the system to be traced to individuals who are held responsible for their actions while using the ILSS. Auditing of Livescan transactions is accomplished by passing the pertinent data to the IDENT1 bureau with each transaction. Auditing of other ILSS user activities, such as creating user accounts, is done through a message interface, as defined in the IDENT1 Livescan Interface Specification.

CC024 All data capture, processing, transformation and handling operations shall be logged.

CC025 The system audit, management and charging facilities shall accurately attribute and report all Livescan transactions.

CL098 The ILSS shall audit each logon attempt by recording the user name, date, time, workstation identifier, and success or failure.

CL099 The ILSS shall audit all security related events, defined as Log-on attempts; Log-outs; creation of Ten Print and Live-ID transactions; and deletion of Ten Print records.

CL151 The ILSS shall audit the creation, modification, and deletion of user accounts to include the action performed, the date/time, the user ID, and the user's actual name.

CL152 The ILSS shall audit each fingerprint capture session, logging who took the fingerprints, the IDENT1 form identification number, the Livescan workstation they were taken on, and the date/time of fingerprinting.

CL154 The ILSS shall audit failed transaction transfers to IDENT1.

CL100 The ILSS shall protect the audit trail from modification, unauthorised access, or destruction.

CL155 The ILSS shall provide audit data in the message formats specified in the IDENT1 Livescan Interface Specification.

CL101 The ILSS audit trail shall be maintained on-line for a period of 3 months.

4.6.4 Interface Requirements

Firstly, there are requirements for interconnecting each instance of the ILSS with the respective IDENT1 Bureau. These requirements depend on the method of communication implemented.

CL102 The connection between the ILSS and a respective Bureau shall be authenticated to prevent unauthorised users from accessing the system, if it is relevant to the communications method used.

Secondly, there are external interface requirements:

4.6.4.1 NSPIS Custody to IDENT1 Livescan

NCNL.01 IDENT1 Livescan shall receive and display detention log information from NSPIS Custody.

NCNL.02 NSPIS Custody shall receive and display IDENT1 identification results.

NCNL.03	NSPIS Custody shall send detention log data to IDENT1 Livescan when a detainee is transferred for fingerprints and palmprints.
NCNL.04	IDENT1 Livescan shall populate demographic data fields with the received detention log data .
NCNL.05	IDENT1 Livescan shall send NSPIS Custody IDENT1 Live-ID, Print-to-Mark, and IND search results for records that received detainee data from NSPIS Custody.
NCNL.06	NSPIS Custody shall send an ASN to IDENT1 Livescan when a detainee is charged.
NCNL.07	IDENT1 Livescan shall populate the Arrest Summons Number (ASN) field of the detainee record with the data received from NSPIS Custody.
NCNL.08	After IDENT1 Livescan is notified that a suspect is charged, Livescan shall automatically send IDENT1 the fingerprints, palmprints, and arrest data of the arrestee to be filed in the IDENT1 national ten print collection.
NCNL.09	NSPIS Custody shall notify Livescan when a detainee is not charged or is released.
NCNL.10	After IDENT1 Livescan is notified that a suspect is not charged, Livescan shall automatically send the detainee fingerprints, palmprints, and arrest data to be printed as a IDENT1 suspect set.
NCNL.11	After IDENT1 Livescan is notified that a suspect is bailed, Livescan shall retain the detainee fingerprints, palmprints, and arrest data until the detainee disposition is determined by Custody.
NCNL.12	IDENT1 Livescan shall not allow changes to the data received from Custody.

4.6.4.2 Immigration and Nationality Directorate (IND) to IDENT1 Livescan

This interface is also known as PIFE - The Police and Immigration Fingerprint Exchange.

PIFE.01	Force Fingerprint Officers (FPO) will perform verification of IDENT1 initiated IAFS print to print searches.
PIFE.02	Force Fingerprint Officers (FPO) will perform verification of IAFS print to mark searches run in conjunction with IAFS initiated print-to-print search requests.
PIFE.03	IDENT1 will perform print-to-print searches initiated by IAFS.
PIFE.04	For IAFS initiated print-to-print searches, IDENT1 will also perform National print to mark searches against the unidentified marks database and Serious Crime Cache.
PIFE.05	IDENT1 will not retain the enquiry ten print records received from IAFS.
PIFE.06	Requirement deleted.
PIFE.07	Requirement deleted.

PIFE.08	IAFS searches can be requested in combination with IDENT1 print-to-print searches or as separate searches.
PIFE.09	The response from a IDENT1 initiated search of the IAFS database will be listed in the IDENT1 bureau's Ten Print Management Queue.
PIFE.10	IAFS initiated print-to-print search requests will be processed by IDENT1 without any required action or review by Police Force Fingerprint Officers.
PIFE.11	Any respondents resulting from an IAFS generated print to mark search will be processed through the IDENT1 compare stage.
PIFE.12	Print to mark search compares will be done by FPOs at the owning bureau of the mark in the first position on the respondent list. PIFE.13 IDENT1 will convert IAFS WSQ formatted images to the IDENT1 JPEG format.
PIFE.14	IDENT1 will convert IDENT1 JPEG formatted images to IAFS WSQ format.
PIFE.15	IDENT1 and IAFS search request and response messages will be formatted using the Interpol 'INT 4' Implementation of the Data Format for the Interchange of Fingerprint Information (ANSI/NIST-ITL 1-2000).
PIFE.16	Police Officers and other authorised Users will be able to request IAFS searches from Livescan workstations in combination with Live-ID requests. The Live-ID/IAFS searches may be verified, non-verified, or use a quoted IFB reference number.
PIFE.17	In response to a Livescan initiated search, two separate response messages will be sent to the Livescan workstation, one for the IDENT1 Live-ID request and one for the IAFS search request.
PIFE.18	When a response from a Livescan initiated search request to IAFS is accompanied by a digital photograph, the Livescan workstation will display the available digital photograph.
PIFE.19	IDENT1 shall provide a request capability for the retrieval, via the IFB form identification number, of IND images. These images may be viewed and printed locally on the IDENT1.
PIFE.20	When a tenprint is placed in a respondent list it shall be possible to print at that bureau all ten finger images from the IAFS tenprint for further comparison purposes. The capability to print such tenprint shall be restricted by User ID. These printouts shall be audited.
PIFE.21	IDENT1 will record the date and time, and source of each IAFS initiated search request, as well as the text data contained in the request.
PIFE.22	IDENT1 will record the date and time, userid, and source of each IAFS search response, and if respondents are included, the ident/non-ident status and demographic data of each respondent reviewed from the response.
PIFE.23	IDENT1 will record the date and time, and source of each IDENT1 initiated search request sent to IAFS, as well as the text data contained in the request.

- PIFE.24 IDENT1 will record the date and time, userid, and source of each IDENT1 search response sent to IAFS, and if respondents are included, the demographic data of each respondent from the response.
- PIFE. 25 The IDENT1 management information system (MIS) will provide a user specified report that gives the counts of IAFS initiated search requests and IDENT1 responses.
- PIFE.26 The IDENT1 management information system (MIS) will include counts of IDENT1 initiated search requests sent to IAFS and IAFS responses.
- PIFE.27 IDENT1 shall perform Ten Print CRO Retrievals initiated by IAFS.
- PIFE.28 IDENT1 will provide a configurable age range filter to limit searches performed by IDENT1. Only subjects within the specified age range will be searched.

4.7 IDENT1 Capabilities

The IDENT1 requirements specify capabilities at the IDENT1 bureau or central segment that incorporate the ILSS functionality. The bureau and central segments interface to the remote Livescan workstation and handle electronic submission, printing, Live-ID search mechanisms, and responses to Custody.

- CL103 IDENT1 shall perform Live-ID and non-verified searches submitted from a Livescan workstation.
- CL104 IDENT1 shall accept electronic ten print submissions from a Livescan workstation.
- CL105 IDENT1 shall handle the search load due to Live-ID search requests submitted from a Livescan workstation up to the limits specified in the IDENT1 Service Level Requirements and other contractual agreements.
- CL106 The IDENT1 Workflow shall support the ten print Livescan and Live-ID transactions submitted from a Livescan workstation.
- CL107 The IDENT1 HCI shall distinguish Livescan submissions from paper submissions when they appear in transaction queues.
- CL108 IDENT1 shall automatically compare the arrest data submitted with a Livescan transaction with the arrest data from PNC/Phoenix. If a match is not made, the user shall be allowed to make corrections utilising the image of the demographic data portion of the Livescan ten pPrint form.
- CL109 IDENT1 shall receive messages from the ILSS. The format and content of these messages is specified in the Livescan IDENT1 Interface Specification.
- CL110 IDENT1 shall send response messages to the ILSS. The format in content of these response messages is specified in the Livescan IDENT1 Interface Specification.
- CL111 The IDENT1 simulation and sizing models shall check the overall impact on the performance due to increased Live-ID submitted from a ILSS workload.

- CL112 The IDENT1 system shall process the maximum workload to the performance levels defined in the SLR from ten print submissions obtained from a mixture of Ten Print forms at bureaux, and remote submissions from the remote service units.
- CL113 The IDENT1 MIS reporting capabilities shall include audit trail reports necessary for the ILSS transactions.
- CL140 The IDENT1 HCI shall distinguish Live-ID transactions from all other transactions.
- CL141 Elimination prints shall be received by IDENT1 and not processed.
- CL142 IDENT1 shall support a P-M search requested through the Live-ID function.

4.7.1 24-Hour Bureau

IDENT1 provides for 24-hour verification of results from searches submitted by the ILSS. During normal business hours, all Livescan transactions are processed by the bureau local to the charging station (Owning Bureau). When the Owning Bureau is closed, Live-ID (print-to-print) and print-to-mark searches can be forwarded to a bureau that offers verification of search results during off hours (24-Hour Bureau). Electronic ten print submissions are queued at the Owning Bureau and processed during the next business day.

- CL156 The IDENT1 server at the Owning Bureau shall be operational 24 hours per day to process the encoding, routing, and auditing of Livescan transactions.
- CL157 A 24-Hour Bureau shall process Live-ID (P-P) and P-M transactions for other bureaux during non-core hours. Non-core hours are defined to be the hours when the Owning Bureau is closed.

APPENDIX A - LIST OF ACRONYMS

AFIS	Automated Fingerprint Identification System
AFR	Automated Fingerprint Recognition
ANSI	American National Standards Institute
A/S	Arrest/Summons
BFES	Bureau(x) Front-End Subsystem
BLAN	Bureau Local Area Network
CDRL	Contract Data Requirements List
CID	Criminal Investigation Department
CONOPS	Concept of Operations
COTS	Commercial off-the-Shelf
CPS	Criminal Print-to-Print Search
CPS	Crown Prosecution Service
CPU	Central Processing Unit
CRO	Criminal Records Office
CSN	Central Segment Network
DPI	Dots Per Inch
FIN	Form Identification Number
FPO	Fingerprint Officer
HCI	Human Computer Interface
IAFS	Immigration and Asylum Fingerprint System
ID	Identification
IFB	Immigration Fingerprint Bureau
IND	Immigration and Nationality Directorate
ILSS	IDENT1 Livescan Subsystem
IOC	Initial Operating Capability
IT	Information Technology
JPEG	Joint Photographic Experts Group

LAN	Local Area Network
LRU	Line Replaceable Unit
MIS	Management Information System
NAFIS	National Automated Fingerprint Identification System
NFO	National Fingerprint Office (“IDENT1 Residual Bureau”)
NIS	National Identification Service
NIST	National Institute of Standards and Technology
NSPIS	National Strategy for Police Information Systems
PIC	Person in Custody
PITO	Police Information Technology Organisation
P-M	Print-to-Mark
PNC	Police National Computer
P-P	Print-to-Print
SLR	Service Level Requirements
SOC	Scene of Crime
UK	United Kingdom
WAN	Wide Area Network

APPENDIX B - GLOSSARY OF TERMS

Please note: To avoid duplication, references to subjects included in IDENT1 Contract Schedule C (**Definitions**) are not included in this Glossary. The IDENT1 glossary contains additional definitions not found in this glossary, which contains only those definitions relevant to the IDENT1 Livescan subsystem.

Acquittal	A form of weeding on IDENT1 due to the dismissal of an offence on an individual's criminal history record. Notice of acquittals will be provided to IDENT1 from PNC/Phoenix.
AFR Codes	An internal format of data describing the features for a single print or mark impression. The AFR Codes are used by the AFR Subsystem to perform print and mark matching functions.
AFR Subsystem	One of the subsystems that comprise the Central Segment. This subsystem provides the Bureaux with Ten Print and mark matching functions and prepares Respondent Lists. It also maintains the IDENT1 repository of Ten Print and mark fingerprint AFR Codes.
Amnesia Set	A set of rolled prints taken from an amnesia victim. The amnesia set is used to help establish the identity of the individual.
Archive	A data storage capability in which fingerprint records are stored for historical purposes. In IDENT1, archives are stored on off-line tape media.
Arrest	The taking or restraining of a Person from his/her liberty.
Arrestee Set	A set of rolled prints taken from an individual that has been arrested and charged with a particular offence.
Arrest Record	A record of a person's criminal activity as applied to a single criminal event. Arrest records are maintained on PNC/Phoenix.
Arrest/Summons (A/S) Number	A unique number, assigned by PNC/Phoenix, to an arrest record.
Automated Fingerprint Identification System (AFIS)	A computer-based method for reading, classifying, searching, matching, and storing fingerprint and related information.
Automated Fingerprint Recognition Subsystem (AFRS)	See "AFR Subsystem".
Backup	A periodic operation performed to make a copy of a data file or a database to ensure its reliability, integrity, and security.

Bureau Local Area Network (BLAN) Subsystem	One of the three subsystems that comprise the Integrated Communications Segment (ICS) of IDENT1. This subsystem provides local Bureau connectivity between BFES hardware components, as well as to the ICS Wide Area Network (WAN) for access to PNC and the Central Segment.
Bureau Manager	See "Head of Bureau".
Bureau Segment	The segment of IDENT1 that contains the Bureau hardware and software. The Bureau Segment contains all of the generalised IDENT1 functions to support the FPO (FPO), the Head of Bureau, and the local Bureau System Administrator. See also Bureau Front-End Subsystem. The baseline IDENT1 design provides ___Bureau Segments to support the Police Forces of England, Wales, the NIS, and Scotland with the capability to expand and provide up to [60] Bureau Segments to support all of the UK.
Bureau System Administrator	A special type of Bureau user who performs in much the same role as the IDENT1 System Administrator, but on a more limited basis. His activities are limited in scope to the system administration functions required at the Bureau.
Candidate	See "Respondent".
Capture	See "Image Capture".
Caution Set	A set of rolled prints taken from an individual that has been arrested and cautioned with a particular offence.
Cell Block	The part of a Custody Office containing individual locked rooms.
Central Image Database	A generic term for the database stored and maintained at the Central Segment and holding the National Ten Print Database and National Unidentified Marks Database.
Central Segment	One of the three segments that comprise the IDENT1 Operational System. This segment is located at the Central Site and serves as the repository of global data and services. It maintains the national databases of Ten Print and unidentified mark images, provides AFR search and match services to all of the Bureaux and the NIS, and provides for the overall control and information flow of all transaction requests and data coming into the Central Site.
Characteristic	Generic term for minutia, core, or delta. Also referred to as Features.

Charge Office	The area within a Custody Office where an arrested person is presented to a Custody Officer and where a PIC is formally charged with the Criminal Offences.
Charging Station	The organisational unit within the local Police Force that processes arrested individuals. A name search using PNC/Phoenix may be conducted at this station to establish a suggested identity or to establish previous criminal history activity.
Charging Station Segment	The IDENT1 segment reserved in the architecture to support optional fingerprint processing functionality at the local level. Options that may be included in the Charging Station Segment are Livescan, Ten Print ID, and Live-ID.
Civilian Support Staff	A person who assists a Custody Officer, sometimes referred to as a Civilian Detention Officer or a Civilian Jailer.
Comparison Print	One of the file fingerprints selected during the matching process. See also Respondent.
Criminal History	A summary of a person's known criminal activity. It includes demographic data concerning the person and previous charges. The criminal history does not include an arrest corresponding to an acquittal.
Criminal History Check	A search of name indexes on PNC/Phoenix to determine whether or not a subject has a prior criminal history.
Criminal Records Office (CRO) Number	A unique number assigned by IDENT1 that is used to identify an individual. A new CRO Number is assigned only if an ident is not found as a result of searching the IDENT1 Ten Print database.
Custody Office	The area where Persons in Custody are held and processed. Referred to often as a custody suite and includes the cell block and charge office. It is an area where movement of 'Persons in Custody' is physically secured by perimeter locked doors and window bars.
Custody Officer	A Police Officer usually of a rank not less than a Sergeant, designated by the Chief Officer of Police, who has the responsibility for the health, well being and the procedures surrounding the detention of a PIC.
Database	A storage scheme for data elements, such as fingerprint characteristics and arrest data. Also refers to the elements stored by the scheme.
Dead Set	A set of rolled prints taken from an unidentified dead body. A dead set is used to help establish the identity of the dead body.

Demographic Data	Non-fingerprint information describing an Arrestee, such as sex, colour, date of birth, etc.
Detainee	See "Person In Custody (PIC)".
Detention	The confinement of a person and the restriction of free movement.
Editing	The manual task of identifying and plotting fingerprint markers (e.g., minutiae, core, delta, etc.) to generate AFR Codes in support of print and mark matching functions.
Elimination Prints	Prints from an Elimination Ten Print Set.
Elimination Set	Shorthand for "Elimination Ten Print Set".
Elimination Ten Print Set	A special type of Ten Print form used to record fingerprints of victims of crime and/or persons who have legitimate access to the scene of crime or articles on which marks are found. Comparisons of these prints with the marks from the case helps to ensure that any remaining unidentified marks are more likely to belong to the perpetrators of the crime.
Enquiry Print	Short-hand for Enquiry Ten Print.
Enquiry Ten Print	The Ten Print that will be compared to file fingerprints in a print-to-print search or a print-to-mark search.
Expandability	Refers to the characteristic of a system that allows new or enhanced functionality to be incorporated without affecting the integrity of the original system design. Contrast with scalability.
Feature	See "Minutia".
File fingerprint	Generic term for a fingerprint stored in one of the fingerprint databases.
Finger Classification	See "Fingerprint Pattern".
Finger Number	The number assigned to each finger on a Ten Print card: starting with the right thumb as 1 and continuing along the right hand to the little finger as 5; the left thumb is 6, continuing along the hand to the little finger as 10.
Fingerprint	A generic term for a single finger impression. Rolled or flat impressions from a Ten Print form are commonly referred to as prints. Partial impressions recovered from a scene of crime are commonly referred to as marks.
Fingerprint Expert	An officer who has served at least five years in a Fingerprint Bureau and has passed the Advanced

	Fingerprint Course at the national training academy to receive an "Expert" status.
Fingerprint Image	A two-dimensional reproduction of the ridge detail of a finger.
Fingerprint Impression	A generic term used to define the lasting imprint left when friction ridges contact an external surface or object. Fingerprint impressions can be made intentionally by rolling inked fingers on a Ten Print form (prints), or un-intentionally by touching a surface and transferring a film of grease or moisture from the friction ridges, thus leaving and outline of the friction ridges (marks).
FPO (FPO)	A generic term for an officer performing fingerprint activities on IDENT1, whether it is scanning, editing, or identification/verification.
Fingerprint Pattern	A classification assigned to fingerprints based on the general shape of their friction ridges. IDENT1 will support four basic fingerprint patterns: Arch (A), Right Loop (\), Left Loop (/) and Whorl (W), as well classifying Unknown (U), Amputee (X) and Missing/Not Printed (N).
Flat Impression	See "Plain Impression".
Form Identifier Number (FIN)	A unique identifier for a Ten Print form that may be pre-printed on the form. The FIN will be comprised of the form type, format, year, and a sequential number.
Force Code	A numeric code used to indicate a particular Police Force.
Form Format	Defines the format or layout of a particular Ten Print form. The form format is used to locate the image/textual areas of a Ten Print form. The Form Identification Number (FIN) will contain an encoded form format.
Form Type	Defines the kind Ten Print form being processed. The form type (e.g., Arrestee Set, Prison Set, Dead Set, etc.) is used to determine the automated processing path for the Ten Print form.
Head of Bureau	A senior FPO who has the responsibility to manage the day-to-day operations of the Bureau and to interact with IDENT1 in order to review common Bureau products and statistics. Also referred to as the Bureau Manager or the Chief FPO.

Human Computer Interface (HCI)	This term applies to all interaction with a computer system required by a user to accomplish a specific task. Specifically for IDENT1, this term applies to all display, keyboard, and mouse actions required by the user to process fingerprint transactions.
Ident	A file fingerprint that has been verified as matching an enquiry print by two or more FPOs in accordance with defined operating procedures. Also, a jargon term for identification.
IDENT1	A distributed computer system that provides the services to maintain the National Fingerprint Collection and the National Collection of Unidentified Marks for fingerprint searching and identification. IDENT1 will be linked to the PNC/Phoenix Criminal Justice Record System.
Identification Officer	FPOs at the National Identification Service and the Metropolitan Police Force (Met) are referred to as Identification Officers.
Immigration & Asylum Fingerprint System (IAFS)	The IAFS system is a database system that contains Fingerprint System (IAFS) fingerprint records and demographic details of asylum seekers.
Immigration Fingerprint Bureau (IFB) Number	A unique number assigned by IAFS that is used to identify an individual.
Immigration and Nationality Directorate Live-ID search type that is available from the Live- (IND)	scan Live-ID from the HCI screen. This search option provides a means to search on the IAFS database.
Image	An electronically processed or stored representation of a fingerprint or mark.
Image Capture	The process by which the system records and stores a visual (physical) representation of Ten Prints, lifts, or marks in electronic form.
Image Enhancement	Computer modification of a fingerprint image to clarify the display of ridge detail for editing or comparison purposes.
Image Scanner	An electro-optical device that converts a two-dimensional image into a digital representation. IDENT1 will support a high-speed scanner for Ten Print forms and a flatbed scanner for SOC lifts/marks.

Integrated Communication Segment (ICS)	One of the four segments that comprise the IDENT1 Operational System. This segment interconnects all of the IDENT1 components through three subsystems: the Central Segment Network (CSN), the Bureau Local Area Network (BLAN), and the Wide Area Network (WAN).
Legal Representative	A solicitor, lawyer or authorised clerk representing a PIC.
Live-ID	An optional capability which allows the Charging Station Workstation to transmit three rolled impressions to the IDENT1 Bureau and to receive an identification response from the Bureau Segment. This capability is integrated with a Livescan Workstation. A future stand-alone Live-ID Workstation will provide only the Live-ID function, and will not require the capture of all ten fingerprints.
Livescan	An optional capability which allows the Charging Station Segment to electronically capture the rolled, plain impressions, and palm impressions, produce a hardcopy Ten Print record, and to send the captured form to a Bureau Segment. Livescan supports two modes of operation — identification and Ten Print submission. (See Live-ID)
Livescan Workstation	The physical device providing the Livescan functions. It includes the chassis, CPU, monitor, keyboard, platens, etc.
Local Area Network	A general term that describes the hardware and software necessary to provide data communications links among computers at the same or nearby geographic locations.
Lossless	A format for preserving fingerprint data such that it can be retrieved without losing any data. Fingerprint data can be compressed at an average ratio of 1.5:1 while preserving complete integrity of the original data.
Lossy	A format for preserving fingerprint data such that it cannot be returned to its original form. Fingerprint data can be compressed in a lossy format at an average ratio of 12:1.
Mark	The accidental reproduction of friction ridge detail on an object when the object is touched (such as at an SOC). Also referred to as a latent.
Match	The process by which the AFR codes an enquiry fingerprint is compared against the AFR codes of file fingerprints to produce a rank-ordered respondent list of file fingerprints most likely to be the mate. Also referred to as "Search".

Match Score	A numerical value assigned to each respondent to a match based on the closeness of match of the enquiry fingerprint to a file fingerprint.
Minutia	A type of Fingerprint Feature where the continuous flow of a single friction ridge is interrupted. A minutia point can be classified as a ridge ending or a bifurcation.
Minutiae	Plural of minutia.
National Fingerprint Collection	Hardcopy collection of Ten Print forms currently maintained by the National Identification Service. Under IDENT1 the National Fingerprint Collection will be distributed and maintained across the Fingerprint Bureaux.
National Fingerprint Image System	Image storage and retrieval system that held the (NFIS) electronic National Fingerprint Collection prior to being converted onto IDENT1 using the BRC System.
National Fingerprint Office (NFO)	The department with responsibility for all Tenprint functions that do not fall to the individual police Fingerprint Bureaux is known as the "IDENT1 Residual Bureau". Part of and also known as the National Identification Service (NIS). With the introduction of IDENT1, responsibility for the National Ten Print Collection devolved to the Bureaux. The NFO has a national audit and inspection role for IDENT1.
NSPIS Custody	National Strategy for Police Identification Systems (NSPIS) Custody will have an optional interface to IDENT1 Livescan units that are co-located at the Police Custody stations. IDENT1 Livescan will receive and display information from NSPIS Custody, and NSPIS Custody will receive and display IDENT1 identification results.
IDENT1 System Administrator	A privileged user who resides at the Central Site. IDENT1 System Administrators do not perform day-to-day fingerprint related functions, but rather perform daily system administration functions on the Operational System, such as creating user accounts, system management, network management, and backup and restore duties.
National Ten Print Collection	See "National Fingerprint Collection".
National Ten Print Database	The IDENT1 Central Segment database containing an electronic version of the National Ten Print Collection.
Non-ident	A determination that two fingerprints or sets of fingerprints do not belong to a particular person, or no mate is found as the result of a search.

Operational System	One of the four systems that comprises the current IDENT1 Architecture. The purpose of this system is to produce idents, help solve crimes, improve productivity and provide end-to-end working capabilities for the fingerprint service.
Owning Bureau	The local IDENT1 bureau that normally processes fingerprint submissions from a custody station.
Palm Print	The impression of the underside of the entire hand.
Pattern	See "Fingerprint Pattern".
Pattern Classification	See "Fingerprint Pattern".
Person In Custody (PIC)	A person who has been arrested or is in a Custody Office as a place of safety and their detention has been authorised by the Custody Officer. Sometimes referred to as a Detainee or Prisoner.
Plain Impression	The impression of all four fingers of each hand taken simultaneously, and of the thumbs, taken without rolling, which appear at the bottom of a Ten Print form. They provide additional ridge detail for comparisons.
Police Force	An organisational unit of law enforcement personnel. A Bureau provides fingerprint services to one or more designated Police Forces.
PITO	Police Information Technology Organisation. The organisation within the UK responsible for Police IT initiatives. Also the Authority for IDENT1.
Print	The electronic representation of an individual impression from a Ten Print set.
Print-to-Mark Search (P-M)	The process of searching a given Ten Print against specified geographic subsets of the National Unidentified Marks Database.
Print-to-Print Search (P-P)	The process of searching a given Ten Print against the National Ten Print Database.
Prison Set	A set of rolled prints taken from an individual either in or entering prison. The prison set is used to establish the identity of the individual.
Processing Thread	A graphical and accompanying textual description of the processing required to execute a particular type of transaction in the system. Processing threads use data flow diagrams to graphically depict the processing flow, and textual descriptions to describe the processing performed at each step in the execution of the transaction.

Respondent	A Ten Print or mark suggested by IDENT1, in response to an AFR search request, as a possible mate.
Respondent List	A rank-ordered list of Ten Print sets or marks suggested by IDENT1 as possible mates to an enquiry.
Rolled Impression	See "Rolled Print".
Rolled Print	A fingerprint impression that has been recorded by rolling the digit 180 degrees from nail edge to nail edge.
Scaleability	Refers to the characteristic of a system that allows it to increase in processing power or storage capacity (to accommodate increases in workload) without affecting the integrity of the original system design. Contrast with expandability.
Scene of Crime (SOC)	The specific place in which a crime was committed.
Score	See "Match Score".
Search	See "Match".
Search Parameters	Parameters limiting the areas of the database that are the focus of the matching process. They may also provide a post match filter to eliminate those respondents unlikely to provide a match on the basis of their associated demographic data.
Segment	A logical part of a system, usually organised in such a way that it represents the configuration associated with a geographic site type.
Service Level Requirements (SLR)	A document that contains reporting mechanisms and procedures that define the service levels to be provided. For IDENT1, Northrop Grumman is the service level provider. The SLR also identifies the Authority's responsibilities as the purchaser, and the Northrop Grumman responsibilities as the supplier.
Station Code	A numeric code use to indicate a particular Charging Station within a given Police Force.
Subsystem	Logical groupings of hardware and software that perform tightly coupled sets of functions.
Suspect Check	A comparison of a suspect set to either prove or disprove an individual's involvement in a crime. Print-to-Print suspect checking can be used to establish an individual's identity. Print-to-Mark or Mark-to-Print suspect checking can be used to establish an individual's involvement in the crime.

Suspect Set	A set of rolled prints taken from an individual suspected of committing or being involved in committing a crime. The suspect set is used to prove a suspect's involvement in the crime or to eliminate a suspect from an enquiry.
System	When used by itself, refers to "IDENT1". IDENT1 is composed of four systems: the Back Record Conversion (BRC) System, the Operational System, the Test and Development System, and the Training System.
Ten Print	Shorthand for "Ten Print Set".
Ten Print Card	See "Ten Print Form".
Ten Print Form	The paper form used at the Charging Station for initially recording a person's fingerprints. Also known as a Ten Print card.
Ten Print ID	An optional capability that allows the Charging Station Segment to electronically capture a Ten Print form and to send the captured form to a Bureau Segment. Ten Print ID supports two modes of operation — identification and Ten Print submission. Ten Print ID is currently not part of the RCSS.
Ten Print Ident	The identity of a set of Ten Prints that has been positively confirmed by FPOs.
Ten Print Set	The set of prints captured from a Ten Print form or captured and received by electronic means.
Ten Print Reference Database	Set of all Ten Prints stored in the Central Image Database in lossless compressed format; primarily stored off-line.
Ten Print Working Database	Set of all Ten Prints stored in the Central Image Database in lossy compressed format for the purpose of fast retrieval.
Thread	See "Processing Thread".
Threshold	A static configuration parameter utilised by software for decision making. In IDENT1, thresholds are used to determine whether a fingerprint requires manual editing or whether a respondent should be included in the respondent list returned to the user. See "Match Score".
Throughput	The number of Ten Print forms, or marks, capable of being processed in a specified time period.

Training System	One of the four systems that comprises the current IDENT1 Architecture. The purpose of this system is to train IDENT1 users to get the best and most efficient use out of the tools and working environment provided by IDENT1.
Transaction	A series of processing steps associated with a specific IDENT1 function.
24 hr. Bureau	A IDENT1 bureau that provides comparison of transaction respondents with enquiries for a custody station, when the custody station's Owing Bureau is closed.
Unique	When referring to data entities, means that the data entity is stored in a single location, and no synchronisation with other data entities is required.
Verification	The process of visually checking and second checking a match using all available image data (e.g., all Ten Print rolled and plain impressions, or all case lifts/marks).
Weeding	In terms of Ten Prints, the removal of a record from the National Ten Print Database based on notification of an acquittal or record deletion (e.g., death, time served, etc.) from PNC/Phoenix. In terms of marks, the deletion of a SOC case or a specific mark from a SOC case stored at a Bureau Segment or the National Unidentified Marks Database. All SOC case and Ten Print weeding requests require approval of the appropriate Bureau authority.
Wide Area Network (WAN)	A general term that describes the hardware and software necessary to provide links among computer systems at different geographic locations.
WAN Subsystem	One of the subsystems in the Integrated Communication Segment (ICS). This subsystem provides the hardware, software, and services to connect the Bureaux to the Central Segment.
Work Flow	A generic reference to the processing, which delivers transactions to processes.