# SCHEDULE Q, PART B

# SYSTEM DESCRIPTION

## CONTENTS

# 1 INTRODUCTION

Schedule Q, Part B (**System Description**) provides a high level description of the Contractor's IDENT1 technical solution at the time of the Effective Date. Subject to Schedule H (**Acceptance Procedures**) and Schedule L (**Change Control Procedures**), as applicable, the final technical solution delivered at FOC and beyond will retain elements of this Schedule, however other parts will evolve and change as part of the agreed development process The technical solution detailed in this Part B shall be superseded through more detailed system documentation as described in Schedule O (**Documentation**) subject to acceptance by the Authority in accordance with Schedule H (**Acceptance Procedures**). These shall include but are not limited to:

- 21 – Configuration Management Baseline
- 37 – Use Case Models
- 42 – COTS Products Register
- 43 – System Architecture Model
- 44 – Conceptual and Logical Data Models
- 45 – Physical Data Models
- 46 – External ICDs
- 47 – Livescan Interface Specification

# 2 THE SYSTEM

IDENT1 is a distributed computer system that provides the services to maintain the national collection of ten-print records and the national collection of marks for fingerprint and palm print searching and identification which is linked to the PNC/Phoenix Criminal Justice Record Service.

The system will be developed by the Contractor to fully meet the requirements of this Contract, in particular Schedule D (**Detailed Operational Requirements**) and to meet the Service Levels detailed in Schedule F (**Service Level Requirements**).

## 2.1 High-Level System Description

Figure 2.1-1 provides a top level architectural view of the IDENT1 System. The System will provide the following

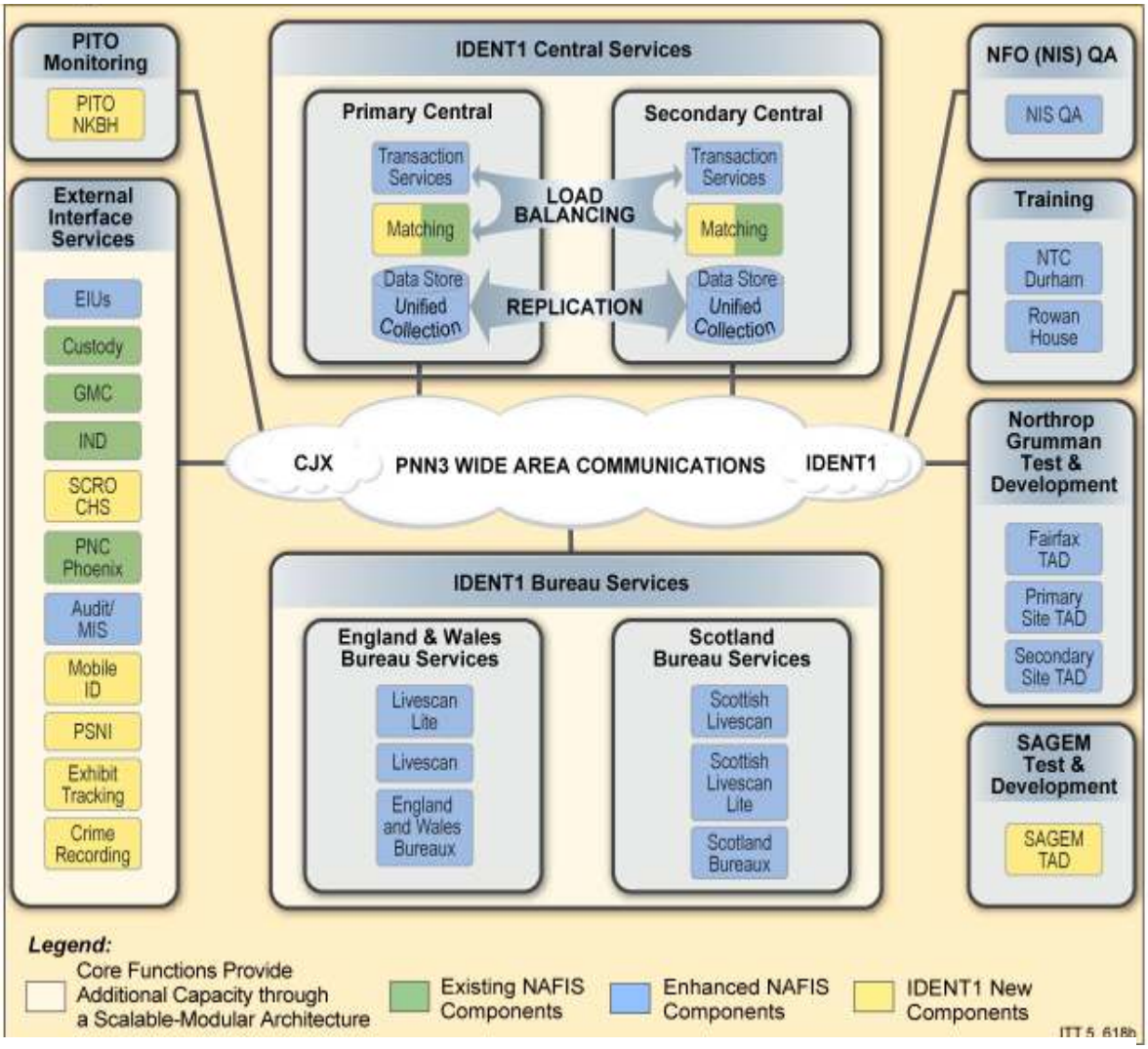



**Figure 2.1-1. Top Level Architectural View: IDENT1 System**

2.1.1 Central Services to include:

(a) searching of marks from local scenes of crime against local, regional and national sections of the ten print and palm print databases (mark to print);

(b) searching of ten print forms against the national ten print database (print to print);

(c) searching of ten prints and palm prints against local, regional and national sections of the marks databases (print to mark);

(d) searching of marks from local scenes of crime against local, regional and national sections of the mark databases (mark to mark);

(e) The Central Services are distributed between primary and secondary sites with high-availability components for load balancing, data replication, and disaster recovery;

(f) Bureau Services at fingerprint bureaux in England and Wales and Scotland, for electronic capture, computerised storage, search and retrieval facilities for both ten print records and scenes of crime (including fraud) marks.

(g) External Interface Services for exchanging data and search requests with other national and international criminal justice and government information systems.

(h) Facilities for the Authority to monitor the System and for the National Fingerprint Office (NFO) to perform quality assurance on business processes, calibrate business value, and measure business improvement.

(i) Training facilities that simulate an operational system bureau, and live-scan, to provide a framework for all training.

(j) Test and development facilities in that mimic the operational system (central, bureau, and live-scan) and provide a framework for all new development.

(k) Network connections within each site (LAN), PNN wide area communications for the transfer of information and images between separate sites (WAN), and to the Criminal Justice Extranet (CJX) for communications with systems outside of IDENT1;

(l) A Plug and Play Architecture that will facilitate incorporation of future requirements for biometrics (such as mug shots or iris scans);

(m) Compliance with current UK standards for interoperability with the UK Criminal Justice infrastructure.

(n) The System will also integrate, manage and maintain data links between ten print records searched and held on IDENT1 with the corresponding records held on PNC and SCRO.

(o) Performance and capacity of the System will be scaleable allowing resources to be added proportionately to meet the anticipated workload as detailed in Schedule F. The System is to be supplied to all the Police Forces of England, Wales and Scotland, and will support further upgrades.

2.1.2 The main functional components of IDENT1 are:

(a) workstations for the input and user processing of all ten print, palm print, and mark work functions;

(b) workstations, required for the formulation and management of search requests, the management and handling of respondents and visual comparison of images for ten print and mark records. Work stations also support other user functional tasks such as monitoring workloads and tasks, preparing exhibits in support of evidential statements and communicating with other personnel using IDENT1.

(c) national databases containing fingerprint images, textual information and data derived from the fingerprints to support AFR

(d) national databases containing palm print images, textual information and data derived from the palm prints to support AFR;

(e) national databases containing scenes of crime mark images, textual information and data derived from the marks to support AFR;

(f) similar local databases to hold work in progress, fingerprint, and palm print information relating to previous submissions of ten prints, palm prints. and marks, and local print image libraries as a subset (image and data) cache of the central image database;

(g) searching and comparison processors for the comparison of fingerprint, palm print, and mark data held in the national or local databases;

(h) specific identified interfaces to other police computer systems, including PNC, SCRO, NCIS, and IND;

(i) production of high quality hard copy (printed to paper) images and textual information as displayed on the screen. This hard copy facility will also include any detail subsequently superimposed by the operator to indicate characteristics which match between the enquiry image and the respondent image, together with any related alphanumeric text;

(j) a national data and information cross reference and tracking database to co-ordinate and log transactions of the national system, and to locate and link all data held by the Bureaux and the central databases;

(k) security facilities for the system

## 2.2 Central Functional Services

The components of the Central functional architecture are shown in Figure 2.2-1.

2.2.1 Central Search Matching performs matching on rolls, flats, and palms using high speed, extensible, parallel processing search engines supporting algorithms and biometrics from multiple vendors.

2.2.2 Central Fusion works in conjunction with matching to increase accuracy and reduce false alarms by combining results from various biometric algorithms.

2.2.3 Central Data Management maintains the National Collection of finger and palm images, biometric features and demographic data, and provides the management for storage and backup of the data. Central Data Management also manages the creation of an off-line archive of fingerprint images in the National Collection.

2.2.4 Central Transaction Services utilizes a J2EE platform to receive, process, and respond to bureau and live-scan transaction requests for searches and database queries.

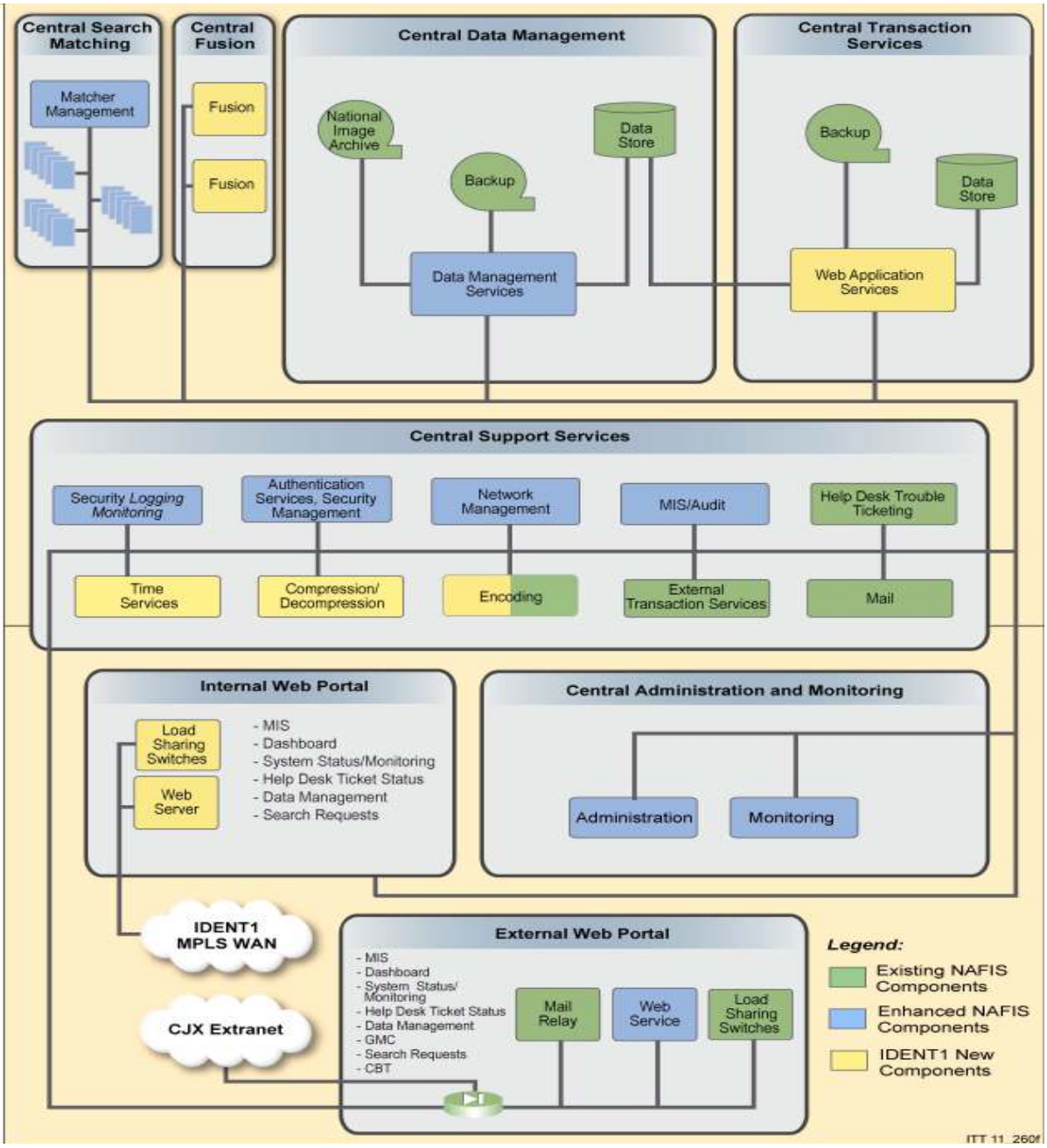



**Figure 2.2-1. Components of Central Functional Architecture**

2.2.5 Central Support Services incorporates the service infrastructure required to support the Central components. Feature encoding and image compression/decompression support the matching component. Email services handle both user messaging and communications with external systems. Security services handle logging monitoring, authentication and audit. HelpService desk and trouble ticket services assist users with system issues. Time services ensure all IDENT1 systems are synchronised to a common clock.

2.2.6 Central Administration and Monitoring provides system administration and monitoring for real-time assessment of system performance and modification of system configuration parameters.

2.2.7 The Internal Web Portal utilizes a Web Server for internal user portal functions and load-sharing switches for Central Transaction Services. The portal gives the user single access to all IDENT1 services including searching, record storage and retrieval, administration, system monitoring, helpdesk functions, and MIS reports. The load-sharing switches direct search requests to multiple Web Service Application machines to balance the system load.

2.2.8 The External Web Portal provides all the services of the Internal Web Portal for users outside the IDENT1 firewall. The NSPIS Custody and the Generic Mark Camera interfaces are also accessed through the external portal. The External Web Portal communicates with Central Transaction Services through a firewall using tightly restricted protocols.

## 2.3 Bureau Functional Services

The components of the Bureau functional architecture are shown in Figure 2.3-1.

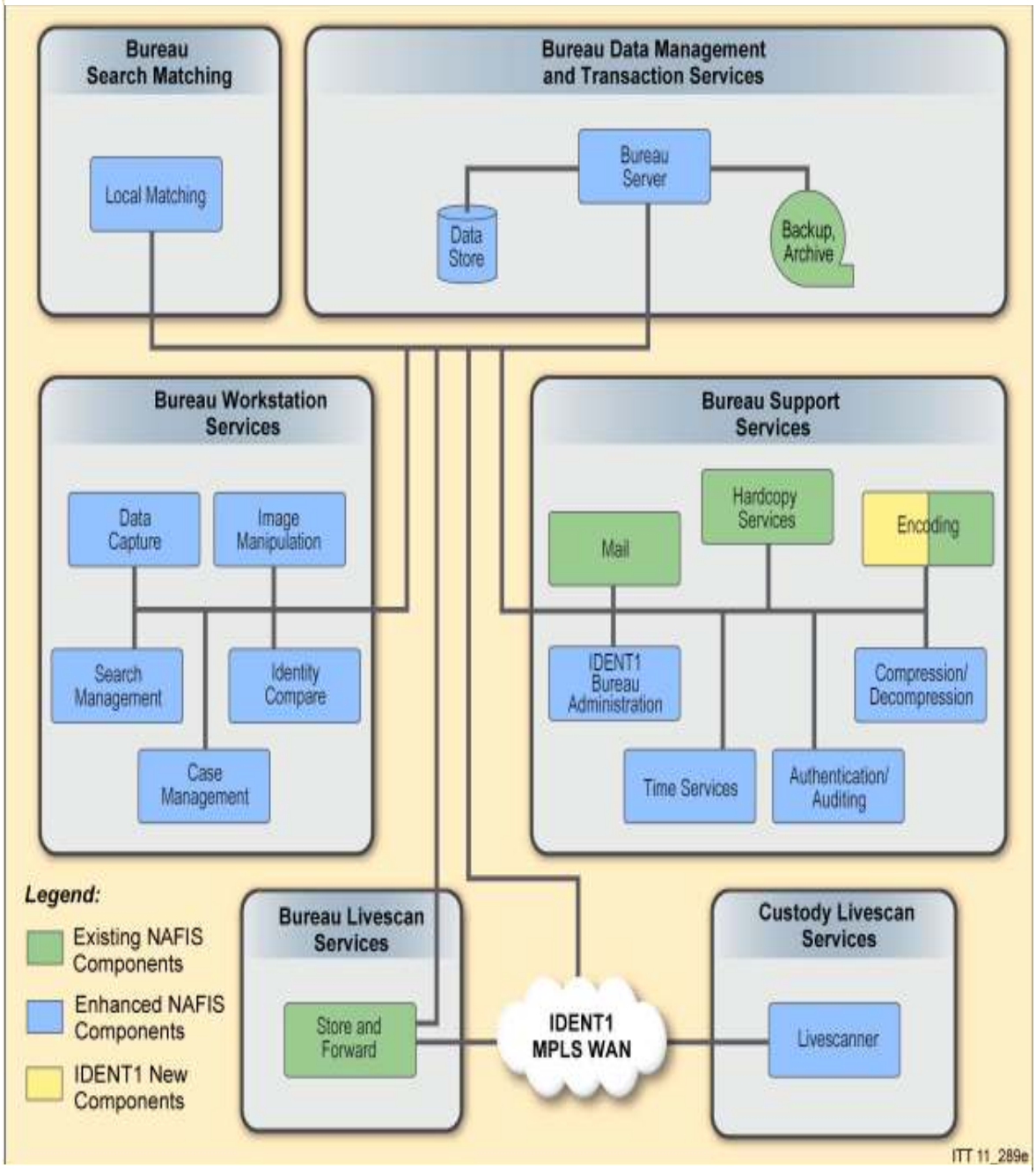



**Figure 2.3-1. Bureau Functional Architecture Components**

2.3.1 Bureau Search Matching encompasses a local AFR search capability and local fingerprint and palm print storage for the bureau local Operational Response and Police Elimination functions. The AFR search capability uses the same technology as Central, with all administrative and monitoring features.

2.3.2 Bureau Workstation Services provide a fast user interface for image capture and manipulation, search, compare, filing and case management.

2.3.3 Bureau Data Management and Transaction Services are Web services accessed by Bureau Workstation Services. Data Management provides standardised interfaces for accessing bureau data, including backup and archive. Transaction Services run the containerised business logic to maintain the current state of each transaction and to guarantee transaction integrity, recoverability and security.

2.3.4 Bureau Support Services provide infrastructure tools for bureau administration, authentication, image encoding, image compression/decompression, office automation, reports, management information, printing, time synchronisation, and email.

2.3.5 Bureau Live-scan Services provide store and forward functions to accept electronic ten print forms for bureau processing from custody live-scan units and to return results.

2.3.6 Custody Live-scan Services provide remote live-scan units for digital capture of fingerprints, palm prints, and demographic data. Live-scan units can initiate search requests including Live-ID against the IDENT1 National Collection and the IND database, Crime Check against the Unidentified Marks Collection, and electronic ten print submission for searching and filing in the IDENT1 National Collection.

2.3.7 Each Bureau will use its own fingerprint staff to input, search, retrieve, compare, verify identity and maintain ten print and mark records. It will be possible for each Bureau to:

(a) handle locally, including AFR searching, the input of ten print sets and mark sequences for routine scenes of crime searches;

(b) access all, or geographically selected, ten print records and marks from national databases held by the system. The geographical search areas may be selected by an operator for each search request;

(c) record the search parameters used so that further searches may take account of previous areas covered and allow suitable audit trails and management information to be retained;

(d) accept fingerprint data (including marks and palm prints) from remote devices, such as: a remote capture station; a paper scanner; a ten print 'live-scan'; a SOC mark electronic camera; on a mobile fingerprint capture device.

## 2.4 External Interface Services

2.4.1 External Interface Services provide the capability to support, as illustrated in Figure 2.4-1:

(a) Search transactions from other agencies (both UK and international).

(b) Data management to synchronise data and keep records up to date throughout the police and criminal intelligence services.

(c) SOAP messages transmitted over the CJX with search requests formatted in ANSI/NIST-ITL 1-2000, Interpol Implementation Version 4.

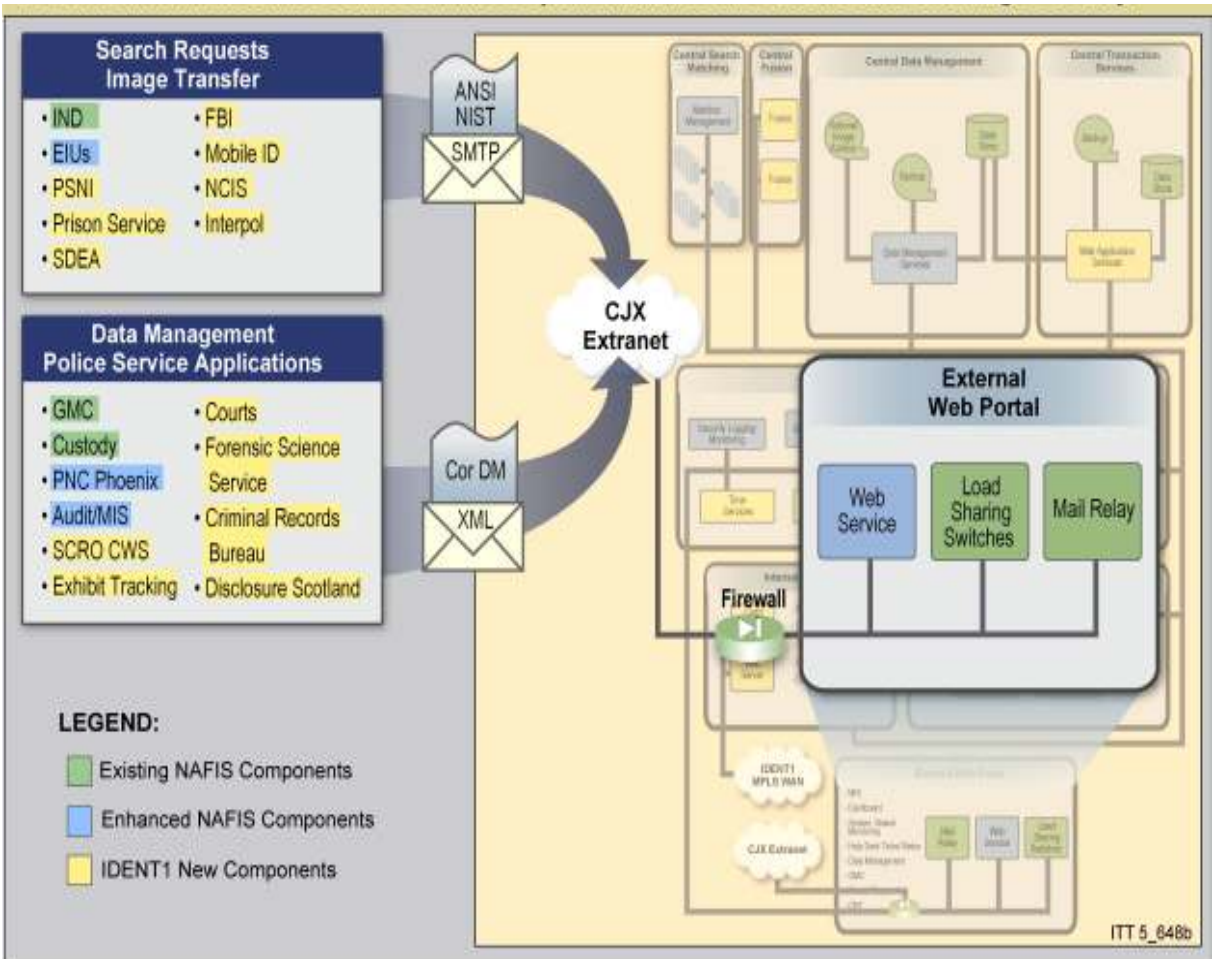



**Figure 2.4-1. External Interface Services**

(d) SOAP messages transmitted over the CJX for data interchange conforming to the corporate data model (CorDM), packaged in XML.

(e) Systems that do not follow the CorDM using XML or ANSI/NIST over the CJX can be assessed for external communications in conjunction with the Authority.

(f) Security requirements employing AAA (authentication, authorisation, and accounting) access control to maintain the RESTRICTED status of IDENT1.

## 2.5 Test and Development Facilities

2.5.1 The Test and Development (TAD) facilities mimic the operational system and provide a framework for evaluation, integration, and upgrades of computer equipment and software.

2.5.2 The TAD will support formal acceptance testing of deliverables, witnessed by the customer.

2.5.3 The TAD includes main server computer systems, network backbone, RAID, backup devices, UPS, user workstations, scanners, printers, live-scan, spares and consumables.

2.5.4 The TAD will support HCI usability trials and rapid prototyping of new capabilities.

## 2.6 Training Facilities

2.6.1 The training facilities provide a complete emulation of the operational system (central and bureau) and provide a framework for all training.

2.6.2 The training facilities are located at the Metropolitan Police Fingerprint Training School, Hendon, the NTC for Scientific Support to Crime Investigation in Durham, and a future third location at Wyboston.

# 3 VIEWPOINTS

Due to the wide range of stakeholders associated with IDENT1, the following sections provide various technical perspectives of the IDENT1 solution. Specifically, the following viewpoints are provided:

- Logical View
- Implementation View
- Distribution View
- Data View
- Physical View

## 3.1 Logical View

This section provides a high level identification of the key business and system entities and their relationships. Figure 3.1-1 depicts a logical view of the domain classes that make up the IDENT1 system. A further textual description of each of the classes and their associations is also provided.

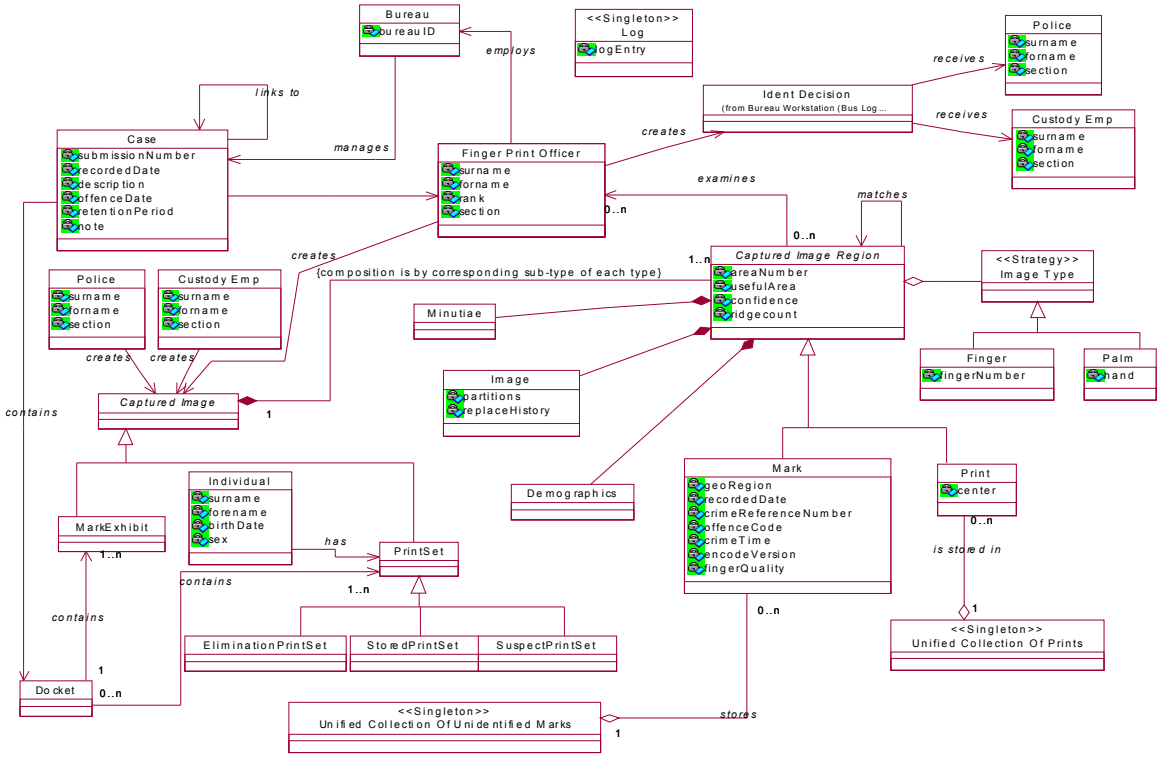



**Figure 3.1-1. IDENT1 Logical View Class Diagram**

### 3.1.1 Bureau

(a) This class represents bureaux in the IDENT1 system. A Bureau is identified by a bureau ID and represents a group of attributes and activities in the system to support bureau system functionality. In the system, each bureau will be identified and have specific cases and finger print officers assigned to it.

(b) **Associations:** A bureau is associated with specific cases that it is responsible for managing, and Finger Print officers which it employs. Each case can relate to multiple cases and multiple finger print officers.

### 3.1.2 Case

(a) Case is a container for information about a crime. It includes general information such as the date of offence, date recorded, and how long it should be kept in the system. Scene of the crime information is kept in the docket associated with each case, including associated print and mark information. Each case is assigned to a bureau.

(b) **Associations:** The Case class has an association with itself. This allows cases to be linked. Cases are associated with bureaus. Multiple cases can be related to a single bureau.

### 3.1.3 Finger Print Officer

(a) The Finger Print Officer class is a system representation of someone who works for a Bureau to process or otherwise manage finger print information. An FPO may be a detainer, an identifier, a data administrator, etc. This class

holds system access information for a specific FPO as well as general information such as name, rank, and section.

(b) **Associations:** Each finger print officer is associated with the bureau that the person being represented works for. There is a many to many relationship with the Captured Image Region class since multiple finger print officers may examine or manage multiple prints and marks. The association between finger print officer and case shows that finger print officers may retrieve and modify case information.

### 3.1.4 Police

(a) The Police class is a system representation of a Police Officer. This class holds system access information for a specific police officer as well as general information, such as name and bureau affiliation.

(b) **Associations:** Authorised police members can submit captured fingerprint images for searching and receive identification information.

### 3.1.5 Custody Employee

(a) The Custody Employee class is a system representation of personnel performing booking activities at custody sites. This class holds system access information for a specific custody employee as well as general information, such as name and bureau affiliation.

(b) **Associations:** Authorised custody employees can submit captured fingerprint images for searching and receive identification information.

### 3.1.6 Ident Decision

(a) The Ident Decision class represents an identification based on the examination of automatically matched fingerprint images. It may contain zero (no-match_or one (positive identification) elements.

(b) **Associations:** Ident Decisions are received by Police and Custody Employee personnel in response to a fingerprint request.

### 3.1.7 Log

This class specifies the Log that records events. There is only one log, and thus is implemented using the Singleton Design Pattern.

### 3.1.8 Captured Image

(a) Captured Image is an abstract super class that holds the common characteristics and behavior of Print Set and Mark Exhibit. It is composed of multiple prints or marks depending on the type of captured image.

(b) Associations: There is a composition association between Captured Image and the Captured Image Region class (prints or marks) where specific prints or marks make up a captured image. If the Captured Image region is deleted from the system there will be a cascading affect and all objects that make it up (prints or marks) will be deleted as well. There are also two inheritance associations; one between Captured Image and Mark Exhibit and the other

between Captured Image and Print Set. Mark Exhibit and Print Set classes are children of Captured Image and inherit common attributes and behavior.

### 3.1.9 Mark Exhibit

(a) A Mark Exhibit represents the system representation of a set of Marks collected from a surface at a scene of a crime. The Mark Exhibit contains individual Marks. The composition association between Captured Image (the parent class or Mark Exhibit) and Captured Image Region implies that a Mark Exhibit is composed of Mark object and deletion of a Mark Exhibit in the system will correspond with the deletion of Mark objects that make it up.

(b) **Associations:** There is an inheritance relationship between Captured Image and Mark Exhibit where Mark Exhibit is the child or "kind" of Captured Image. Mark Exhibit inherits some abstracted attributes and behavior from Captured Image.

(c) There is also an association between the Docket class and Mark Exhibit where the Docket associated with a Case may be associated with multiple Mark Exhibits. In other words a case docket may contain multiple mark exhibits.

### 3.1.10 PrintSet

(a) PrintSet is the system representation of a collection of prints that have been gathered by a print officer. An example is a Ten Print. A PrintSet is produced in a controlled environment, with the individual identified (as opposed to a Mark Exhibit which is discovered at a SOC). The PrintSet is made up of individual prints (finger and palm), which can be compared to other prints or to Marks. The PrintSet contains individual Prints. The composition association between Captured Image (the parent class or PrintSet) and Captured Image Region implies that a PrintSet is composed of Print objects and deletion of a PrintSet in the system will correspond with the deletion of Print objects that make it up.

(b) **Associations:** There is an inheritance relationship between Captured Image and PrintSet where PrintSet is the child or "kind" of Captured Image. PrintSet inherits some abstracted attributes and behavior from Captured Image.

(c) There is also an association between the Docket class and PrintSet where the Docket associated with a Case may be associated with multiple PrintSets. In other words a case docket may contain multiple printsets.

(d) There is a relationship between Individual and PrintSet where Individual contains personal information of someone who has a set of prints in the system.

(e) There is an inheritance association between PrintSet and the three classes; EliminationPrintSet, StoredPrintSet, and SuspectPrintSet. These three subclasses represent different types of PrintSets with unique attributes and behavior.

### 3.1.11 EliminationPrintSet

(a) This class represents a set of prints that belong to a person authorized to be at a scene of a crime or to handle crime scene artifacts, such as an investigating officer or an evidence processor. This set is used to eliminate prints that are known not to belong to the criminal.

(b) **Associations:** There is an inheritance relationship between PrintSet and EliminationPrintSet where EliminationPrintSet is the child or "kind" of PrintSet.

### 3.1.12 StoredPrintSet

(a) This is a print set that has been added to the Unified Collection of Prints

(b) **Associations:** There is an inheritance relationship between PrintSet and StoredPrintSet where StoredPrintSet is the child or "kind" of PrintSet.

### 3.1.13 SuspectPrintSet

(a) This is a print set that is known to belong to an identified suspect. It is used to remove marks that match it from the search, since the identity of the Mark is known from this set.

(b) **Associations:** There is an inheritance relationship between PrintSet and SuspectPrintSet where SuspectPrintSet is the child or "kind" of PrintSet.

### 3.1.14 Individual

This class contains the personal information of the person providing the print set. It is a one to one relation to Print Set, and may be combined into the Print Set class.

### 3.1.15 Captured Image Region

(a) Captured Image Region is an abstract class that contains the common features of a Print and a Mark. There is a corresponding relation from each Captured Image subclass to each subclass of Captured Image Region.

(b) **Associations:** There is a composition association between Captured Image and the Captured Image Region class (prints or marks) where specific prints or marks make up a captured image. If the Captured Image region is deleted from the system there will be a cascading affect and all objects that make it up (prints or marks) will be deleted as well. There are also two inheritance associations; one between Captured Image Region and Mark and the other between Captured Image Region and Print. Mark and Print classes are children of Captured Image Region and inherit common attributes and behavior. There are composition association between Captured Image Region and three classes; Minutiae, Image, and Demographics. That is to say a Captured Image Region is made up of specific Minutiae, Image, and Demographic objects.

(c) The Captured Image Region class has an association with itself. This indicates that captured Image Regions may be matched against other Captured Image Regions.

(d) There is an aggregation relationship between Captured Image Region and Image Type. This indicates that Captured Image Region "has" Image Types.

This is similar to a composition relationship with the exception that Image Type objects making up a Captured Image Region object can survive in the system without the object they are associated with.

(e) There is an association between Finger Print Officer and Captured Image Region since a finger print officer is responsible for examining prints and marks.

### 3.1.16 Image Type

(a) Image Type is a strategy that determines the specific attributes and behaviors related to the two possible image types of Finger and Palm.

(b) **Associations:** There is an inheritance association between Image Type and the Finger and Palm classes.

### 3.1.17 Mark

(a) A Mark is a region of a Mark Exhibit (a print), that has been discovered without an identified individual.

(b) **Associations:** There is an inheritance relationship between Captured Image Region and Mark where Mark is the child or "kind" of Captured Image. Mark inherits some abstracted attributes and behavior from Captured Image Region.

(c) There is an Aggregation association between Unified Collection of Unidentified Marks and Mark where marks are "part of" the single unified collection of unidentified marks.

### 3.1.18 Print

(a) A print is a region of a PrintSet with a known individual that it belongs to. It is obtained by a print officer and has a specific structure, such as a rolled fingerprint or a palm print.

(b) **Associations:** There is an inheritance relationship between Captured Image Region and Print where Print is the child or "kind" of Captured Image. Print inherits some abstracted attributes and behavior from Captured Image Region.

(c) There is an Aggregation association between Unified Collection Of Prints and Print where prints are "part of" the single unified collection of prints.

### 3.1.19 Minutiae

(a) This class contains the feature information that is extracted from a Print or a Mark.

(b) **Associations:** There is a composition association between Captured Image Region and Minutiae. That is to say a Captured Image Region is made up of specific Minutiae objects and deleting the Captured Image Region object will result in deletion of associated Minutiae objects.

### 3.1.20 Image

(a) This class represents the raw data image of the print or mark. The digitized image is stored on disk, and this class provides the link to the image, as well as behavior to store and retrieve it.

(b) **Associations:** There is a composition association between Captured Image Region and Image. That is to say a Captured Image Region is made up of specific Image objects and deleting the Captured Image Region object will result in deletion of associated Image objects.

### 3.1.21 Demographics

(a) This class contains demographic information about the print or mark, including the individual who supplied it, location, time, and conditions when collected, if available.

(b) **Associations:** There is a composition association between Captured Image Region and Demographics. That is to say a Captured Image Region is made up of specific Demographics objects and deleting the Captured Image Region object will result in deletion of associated Demographics objects.

### 3.1.22 Image Type

(a) Both Marks and Prints may be from the finer or from the palm. To avoid multiple inheritance, or parallel inheritance hierarchies, we use the Strategy design pattern to capture the information about the type of image. Differences in behavior depending on the print type, such as feature matching, are captured in the subclasses of this class.

(b) **Associations:** There are inheritance associations between Image Type class and Finger and Palm classes representing the two types of Image Type classes.

### 3.1.23 Finger

(a) This is a print or mark from a finger on the hand. This class represents specific attributes and behavior associated with a Finger type of image.

(b) **Associations:** There is an inheritance association between Image Type and Finger so that there may be specific attributes and behavior related to fingers.

### 3.1.24 Palm

(a) This is a print or mark from the palm of the hand. This class represents specific attributes and behavior associated with a Palm type of image.

(b) **Associations:** There is an inheritance association between Image Type and Palm so that there may be specific attributes and behavior related to palms.

### 3.1.25 Unified Collection of Unidentified Marks

(a) There is only one Unified Collection Of Unidentified Marks, which contains Marks that have been gathered by investigating officers, but have not yet been matched, and identified as unidentified by a Finger Print Officer.

(b) **Associations:** There is an Aggregation association between Unified Collection Of Unidentified Marks and Mark where marks are "part of" the single unified collection of unidentified marks.

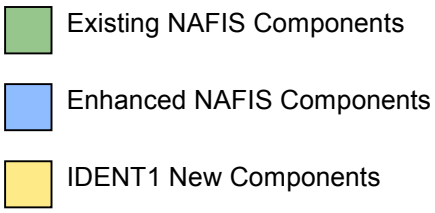
3.1.26 **Unified Collection of Prints**

(a) There is only one Unified Collection of Prints, which contains all of the identified prints that have been gathered and stored in the system. It corresponds to the unified collection print database.

(b) **Associations:** There is an Aggregation association between Unified Collection Of Prints and Print where prints are "part of" the single unified collection of prints.

## 3.2 Implementation View

Figure 3.2-1 provides a UML representation of the implementation view of IDENT1 Central Services. Lower level components are shown grouped into packages, and each component is colour coded to indicate existing NAFIS components (green), enhanced NAFIS components (blue), and IDENT1 new components (gold).




Dependencies are used to represent major communication paths between the packages. As shown in the figure, all packages communicate with the Central LAN package to make use of network services.

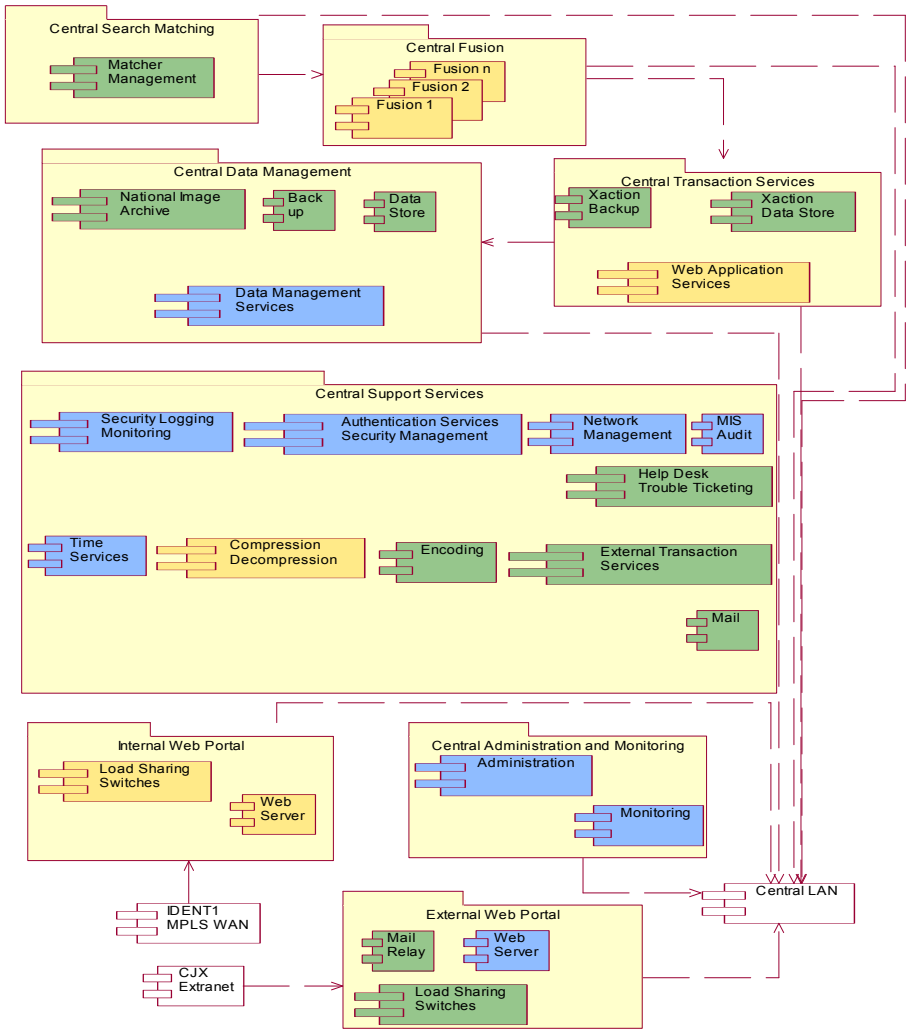



**Figure 3.2-1. Central Services Component Diagram**

Central Services is made up of eight high level components: Central Transaction Services, Central Search Matching, Central Fusion, Central Data Management, Central Support Services, Central Administration and Monitoring, Internal Web Portal, and External Web Portal. Each of these components and corresponding sub components are discussed below.

### 3.2.1 Central Transaction Services

Central Transaction Services is responsible for receiving, processing, and responding to fingerprint and palm match, update and delete requests. This package receives requests from bureaus and is able to satisfy those requests with direct connections to Central Fusion to provide matching functionality, and Central Data Management to modify stored data and images, and return images related to matches. This package is made up of three major components including a transaction data store and back up, and a Web Application Services component that hosts the search services.

### 3.2.2 Central Fusion

The Central Fusion package responds to match requests received from the Central Transaction Services component by requesting matches from Central Search Matching component to obtain match results and fusing results from multiple matching algorithms for increased accuracy. The Central Fusion package is made up

of multiple Fusion components that contain intelligence on how various matching algorithms interact.

### 3.2.3 Central Search Matching

The Central Search Matching package is responsible for distributed matching where matches are processed in parallel by multiple COTS search engines. The Matcher Management component provides automated management for distributed matching. Match results are returned to the Central Fusion package.

### 3.2.4 Central Data Management

The Central Data Management package is responsible for providing services to manage the National Collection database including archiving and data backup functionality as well as image, feature, and demographic data retrieval and update. This package is connected to the Central Transaction Service package in order to provide data for match results and to perform adds, updates, and deletes of image, feature and demographic data. Components include the National Image Archive, the National Collection Data Store and Backup, which contain image, biometric feature, and demographic data. A fourth subcomponent, Data Management Services, is responsible for handling management of the other three subcomponents.

### 3.2.5 Central Support Services

The Central Support Services package provides the infrastructure to support the other Central Services components. Security services are provided by the Security Logging, Monitoring, Authentication Services Security Management, and MIS Audit components. Other components that provide support functionality include Network Management, Help Desk Trouble Ticketing, Time Services, Compression/Decompression, Encoding, External Transactions Services, and Mail

### 3.2.6 Central Administration and Monitoring

This package is responsible for the system administration and monitoring of the entire Central system. The Monitoring component tracks the status of monitored items in each machine. The other component is Administration.

### 3.2.7 Internal Web Portal

This package provides access for internal users of the Central system. The Load Sharing Switches component directs requests for the Central Transaction Services package to Web Service applications machines that handle requests in a load-balanced fashion. The Web Server component provides a portal to all Web-enabled applications available at Central. Access to the Internal Web Portal package will come from the connection to the IDENT1 MPLS WAN as shown in the component diagram.

### 3.2.8 External Web Portal

This package provides access to external users outside the IDENT1 firewall. This access is provides with a connection to the CJX Extranet. The Load Sharing Switches component also provides distribution of requests for Central Transaction Services. This package, like the Internal Web Portal package, provides access to Web-enabled applications at Central.

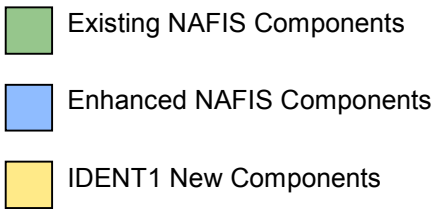



Figure 3.2-2 provides a UML representation of the implementation view of IDENT1 Bureau Services. Lower level components are shown grouped into packages, and each component is color coded to indicate existing NAFIS components (green), enhanced NAFIS components (blue),and IDENT1 new components (gold). Dependencies are used to represent major communication paths between the packages. As shown in the figure, all packages communicate with the Bureau LAN package to make use of network services.

Bureau Services is made up of six high level components; Bureau Data Management and Transaction Services, Bureau Search Matching, Bureau Workstation Services, Bureau Support Services, Bureau Livescan Services, and Custody Livescan Services. Each of these components and corresponding sub components are discussed below.

### 3.2.9 Bureau Data Management and Transaction Services

This package provides services to be accessed by the Bureau Workstation Services package. Data management includes standardized interfaces to access data on the Bureau server and functionality to store and archive data generated at the Bureau (cases, images, demographics, etc.) as well as data sent to the Bureau from the central site (e.g. fingerprint images for comparison). Transaction services are provided to maintain transaction integrity and to maintain the state of ongoing Bureau transactions. It connects to the Bureau Workstation Services to provide data to support workstation functionality such as edit and compare. It connects to the Bureau Search matching to provide case, fingerprint, and mark matching. Comp9onents include Bureau Server, Data Store, and Backup Archive.

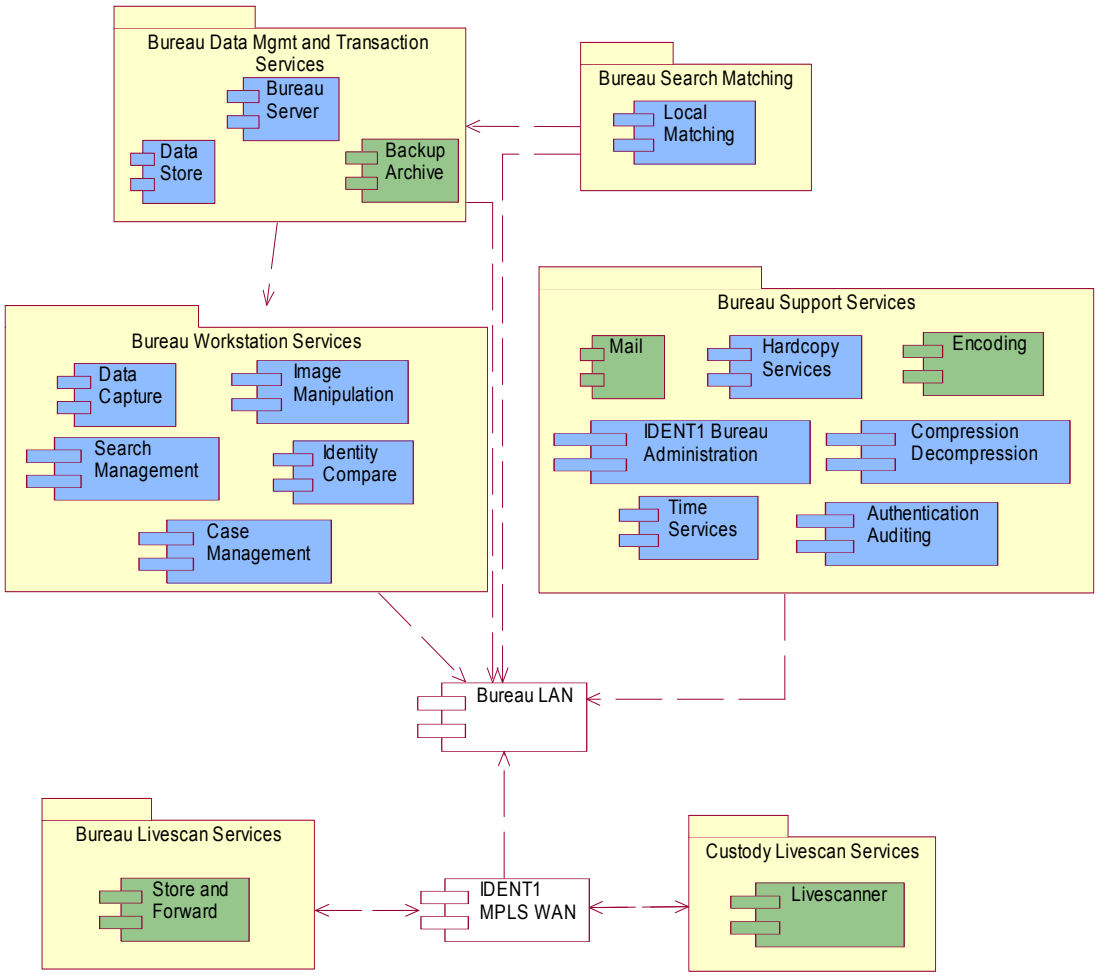



**Figure 3.2-2 Bureau Services Component Diagram**

### 3.2.10 Bureau Search Matching

This package provides fingerprint and palm storage and search functionality. The Local Matching component provides the main capability of automated management for distributed matching at the Bureau level. Match results are returned to the Bureau Data Management and Transaction Services package.

### 3.2.11 Bureau Workstation Services

This package represents the user interface to invoke services on the Bureau server as well as subcomponents that allow certain activities to be performed in order to support Bureau activities. The Data Capture and Image Manipulation components provide capability of recording marks and prints and manipulating images prior to matching or Identify and compare. The Search Management component supports functionality required to handle match requests. The Identify Compare and Case Management components support recording compare results and updating Case information at the Bureau.

### 3.2.12 Bureau Support Services

The Bureau Support Services package provides the infrastructure to support optimal performance and security for the Bureau system. The Bureau Authentication Auditing component provides security support for the Bureau. The IDENT1 Administration

component represents tools to help optimize system performance. The encoding and Compression/Decompression components provide functionality for Image encoding and compression utilizing distributed processing. Other components include Mail, Hardcopy Services for Printing, and Time Services.

### 3.2.13 Bureau Livescan Services

This package and its main Store and Forward component provides Store and Forward services to accept remote electronic ten print forms from custody Livescan units for processing at the Bureau.

### 3.2.14 Custody Livescan Services

This component package provides the ability to scan a ten print and submit a ten print form with accompanying demographic information to the Bureau for print matching.

## 3.3 Distribution View

The Distribution View shows the physical location of hardware and software components at the three primary types of sites planned for IDENT1. The hardware and software at the Primary Central Site support the storage, maintenance and searching of the National Unified Mark and Ten Print Databases. The hardware and software are duplicated at a Secondary Site to provide fail-over recovery, but in normal operation these assets are also used to support day-to-day processing.

The majority of the hardware and software components at the bureau sites, such as workstations and scanners, provide the human computer interface for IDENT1 users. In addition, bureau sites contain a downsized version of the hardware and software provided at the Central Site to perform local storage, maintenance and searching of site specific datasets such as ORD. While it is possible to locate the bureau functionality at the Central Site without significantly affecting the architecture, providing a distributed, two-tiered distribution of hardware and software reduces required WAN bandwidth, improves user response time and facilitates the provision of specialized bureau specific functions.

Custody sites contain the hardware and software components required to provide the human computer interface to capture ten print images and data and receive match results. The fingerprint search processing for the custody site is performed at the bureau or Central site, depending on the type of match request.

Figures 3.3-1 and 3.3-2 are figures extracted from the Northrop Grumman proposal which focus on two different aspects of IDENT1 system distribution. While both figures depict the same software components (Data Delivery, Access Control, Transaction Management, etc), Figure 3.3-1 is a UML representation of the allocation of the software components to hardware at the Central and Bureau sites. It depicts each of the hardware components and lists the software components that will be deployed on each hardware platform. Figure 3.3-2 is a structured representation that focuses on the source of the software components (existing NAFIS, enhanced NAFIS, COTS or new components). It also reflects some of the high level relationships between the software components. For example, the Application Server component “contains” the SOAP Interface, Transaction Management and Match Fusion components.

The following section describes each of the hardware and software components depicted in the two figures.

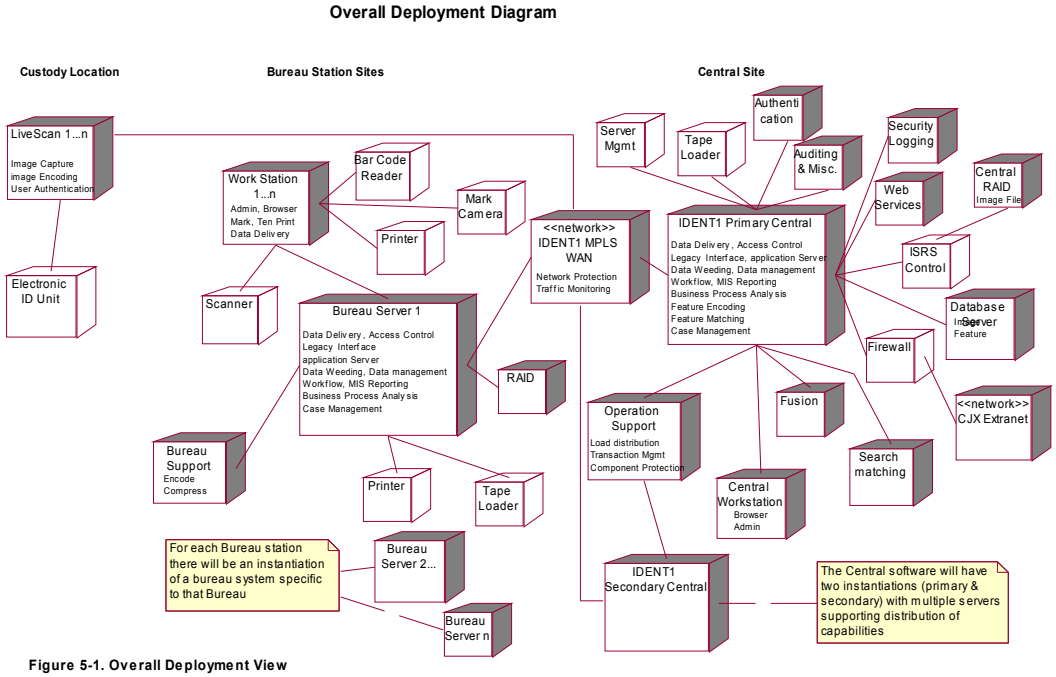



Figure 5-1. Overall Deployment View

**Figure 3.3-1. Overall Deployment View**

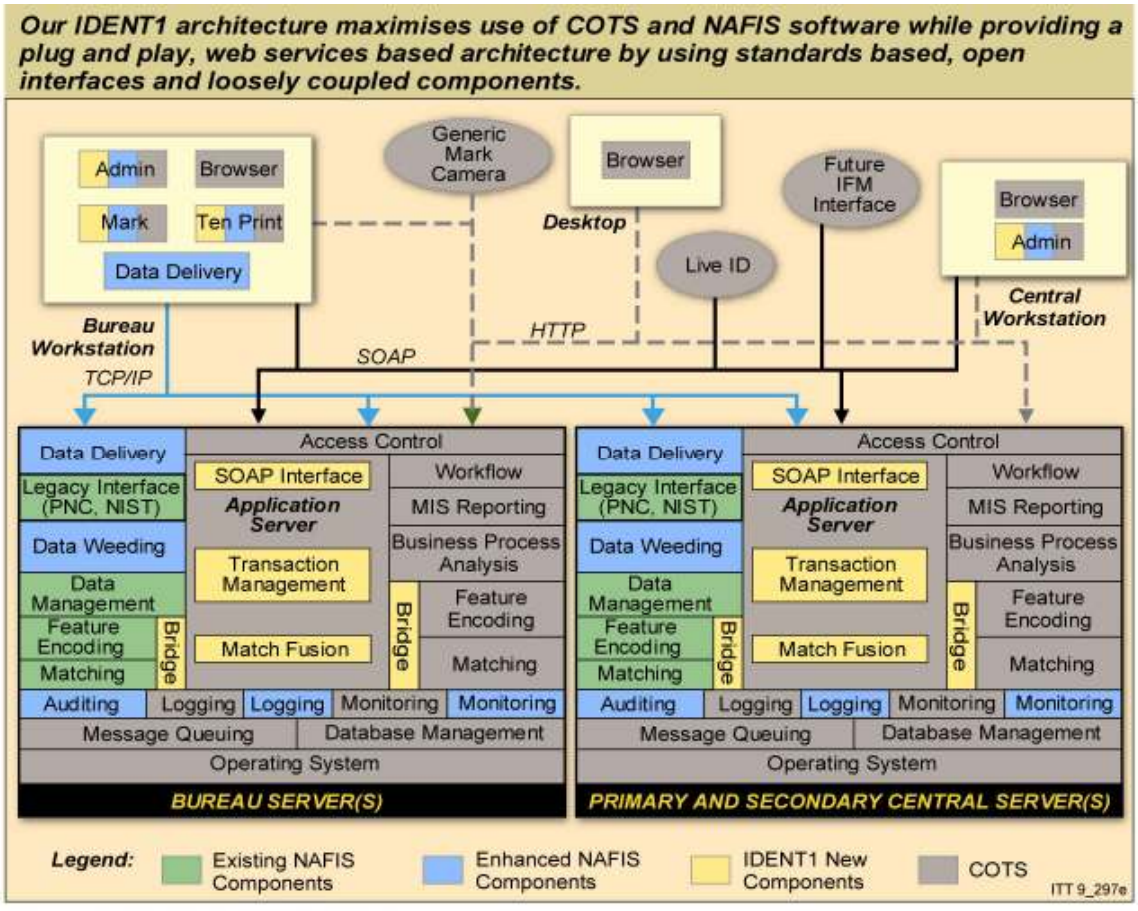



**Figure 3.3-2. Software Architecture**

### 3.3.1 Custody Location

The custody location type represents a location where a person is being detained. This can be a jail or some other remote location. The following processors and devices may be located at a given custody site.

**Livescan:** There will be multiple Livescan units that automate the process of reporting persons in custody. Ten print forms are electronically generated and sent to a Bureau site or the Central system for processing for an identity check. Access to the Bureaux or Central systems is through the IDENT1 MPLS WAN. The main functionality identified to support this capability includes Image Capture, Image Encoding, and User Authentication.

**Electronic ID Unit:** This is a device attached to the Livescan unit that allows the scanning of prints into the Livescan system.

**IDENT1 MPLS WAN:** This is the network that connects Livescan units, Bureaux, and the Central system. Applications/components that support the network include Network Protection and Traffic Monitoring.

### 3.3.2 Bureau

Each bureau has a separate location with its own hardware and software. The following processors and devices are the typical ones for a Bureau.

**Bureau Server:** There will be at least one instantiation of a Bureau server for each Bureau location. These servers will be responsible for local storage, maintenance and searching of site specific datasets. Many of the same applications that run at the Central Site will also run at the Bureau sites. These include:

(a) Data Delivery is used for the transport of large volumes of data between Bureau server and the workstations and Central servers.

(b) Access control provides authentication of users and external devices.

(c) Legacy Interface enables communication with legacy components.

(d) Application Server is used to handle requests for Bureau services. Transactions are parsed, translated and scheduled based on workflow rules for each transaction type.

(e) Data Weeding is used to delete records related to an individual from the system based on specified weeding and retention rules.

(f) Data Management handles the organization, retrieval, and modification of bureau data.

(g) Workflow ensures the proper sequencing of transaction is followed for given service requests.

(h) MIS reporting is a COTS application that handles reporting on system activity.

(i) Business Process Analysis is a COTS tool that supports the simulation and analysis of business process workflow.

(j) Feature Matching allows local bureau systems to handle requests for local print and mark matching against bureau specific data.

(k) Case Management supports capabilities to manipulate case information at the bureau systems.

**Bureau Support:** Bureau support contains the major components that provide system support including feature encoding and compression. Feature Encoding provides image encoding capability on the bureau systems.

**RAID:** This is a disk farm that provides high-availability, and recoverable data storage.

**Tape Loader:** Each Bureau system will have a tape loader to perform backups and archiving.

**Printer:** Each Bureau system will have at least three printers tied to it, a test printer, a colour graphics printer, and a high quality printer for printing fingerprint images.

**Workstation:** There will be multiple Bureau workstations at each bureau location that will act as a user interface to services provided by the bureau system and will also perform some business logic functionality such as image capturing, encoding, case scanning, and image enhancing. Applications/components running on a workstation include:

(a) Data Delivery is used for the transport of large volumes of data between Bureau server and the workstations and Central servers.

(b) Administration coordinated activities on a bureau workstation including case management.

(c) Browser is used for user interface access to the bureau system.

(d) Mark encompasses the components and applications that allow a Finger Print Officer to scan, encode, enhance, compare, and manage mark images.

(e) Ten Print encompasses the components and applications that allow a Finger Print Officer to scan, encode, enhance, compare, and manage fingerprint and palm images associated with a ten print form.

Bar Code Reader: This device will be used in case management to identify dockets and other artifacts associated with a case.

Mark Camera: This device will be used to capture scene of the crime marks and input them into the bureau workstation.

Scanner: There are two types of scanners provided: a high-speed double-sided ten print scanner and a flatbed single-sided mark scanner.

Printer: Printer devices will be available for bureau workstations.

### 3.3.3 Central Site

The central site consists of two identical systems located at a primary and a secondary site. The hardware and software at the Central Site support the storage, maintenance and searching of the National Unified Mark and Ten Print Databases. The hardware and software are duplicated at a Secondary Site to provide fail-over recovery, but in normal operation these assets are also used to support day-to-day processing. The following processors and devices represent the makeup of the Central Site.

**IDENT1 Primary Central:** This represents a set of servers that support the day-to-day processing and support of mark and print searching at the national level. Many of the same applications that run at the Central Site will also run at the Bureau sites. These include:

(a) Data Delivery is used for the transport of large volumes of data between Bureau server and the workstations and Central servers.

(b) Access control provides authentication of users and external devices.

(c) Legacy interface enables communication with legacy components.

(d) Application Server is used to handle requests for Central services. Transactions are parsed, translated and scheduled based on workflow rules for each transaction type.

(e) Data Weeding is used to delete records related to an individual from the system based on specified weeding and retention rules.

(f) Data Management handles the organization, retrieval, and modification of central data.

(g) Workflow ensures the proper sequencing of transactions is followed for given service requests.

(h) MIS reporting is a COTS application that handles reporting on system activity.

(i) Business Process Analysis is a COTS tool that supports the simulation and analysis of business process workflow.

(j) Feature Encoding provides image encoding capability on the central system.

(k) Feature Matching allows local the central system to handle requests for local print and mark matching against central data.

(l) Case Management supports capabilities to manipulate case information at the central system.

**Authentication:** This process provides security for user authentication and authorization.

**Auditing and Misc.:** This process handles system auditing support.

**Security Logging:** This is a security feature that logs and reports system activity.

**Web Services:** The system is set up as a service oriented architecture that employs web services. This processor holds many of the web services components.

**Database Server:** The database server contains the feature and demographic data as well as pointers to related images on the Image database handled by the ISRS controller.

Feature minutiae derived during encoding are stored in the feature database. There will be feature databases to support the primary and secondary Central systems.

The Image data includes images and demographics related to images.

**ISRS Control:** This device provides access to RAID storage containing image files.

**Fusion:** Fusion is made up of multiple Fusion components that contain intelligence on how various matching algorithms interact. These may be distributed across multiple servers.

**Search Matching:** Search Matching is responsible for distributed matching where matches are processed in parallel by multiple COTS search engines. Search engines will be distributed across multiple servers for load balancing.

**Central Workstation:** The central workstation is a thin client that is used primarily as a user interface to the central system. It contains a Browser for user interfaces and an administration component that coordinates activities on a central workstation.

**Operation Support:** This processor coordinates support between the primary and secondary central systems. It is responsible for providing services such as load distribution, transaction management, component protection, and failover coordination.

**Firewall:** This device is used as a layer of security between the CJX Extranet and the central system.

**CJX Extranet:** This represents the external network connection to the central system.

**Ident1 Secondary Central:** This is a duplicate do theIDENT1 Primary Central system whose main purpose is to back up the primary system for failover recovery and also provides support for day-to-day processing under normal condition.

### 3.3.4 Technical Standards Applicable to IDENT1

**Simple Object Access Protocol (SOAP)**

- By the end of the first year of the contract, SOAP will be used as the interface protocol to transfer search requests and results between the Live Scan units and the Central Site. It will also be used to implement the "gateway" interface between the Application server and applications that will be reused from NAFIS such as feature extraction and matching.
- By FOC, SOAP will be used as the interface protocol to transfer search requests, results and respondent lists between the Bureau and the Central Site.
- After FOC, it is envisioned that SOAP will be used to provide fingerprint matching as a web service to CJS shareholders.

**Universal Description, Discovery, and Integration (UDDI)**

- Post FOC, UDDI will provide the mechanism for CJS shareholders to find and interface with the fingerprint matching web service provided by IDENT1.

**Web Services Description Language (WSDL)**

– By the end of the first year of the contract, WSDL will be used to specify the SOAP structures and interfaces used to transfer search requests and reposnes.

– After FOC, WSDL will be used to create the UDDI description of the fingerprint matching web service.

**Java 2 Platform, Enterprise Edition (J2EE)**

– By contract award, J2EE will be used as the standard for developing the component based, multi-tier enterprise applications that will implement the new IDENT 1 functionality.

**Structured Query Language 2 (SQL2)**

– By FOC, SQL 2 will be used as the query language used to implement database adds, inserts, queries and deletions for new IDENT1 database applications.

**Transmission Control Protocol/Internet Protocol (TCP/IP)**

– By contract award, TCP/IP will be used as the network protocol for transferring data across the Wide Area and Local Area networks.

**Simple Mail Transfer Protocol (SMTP)**

– By contract award, SMTP will be used to transfer email messages between CJS stakeholders over the CJX network. Email over SMTP is also used to receive ANSI/NIST–ITL 1-2000 Version 4.20 formatted messages from external entities for subsequent processing.

**Simple Network Management Protocol (SNMP)**

– By contract award, SNMP will be used to collect status and performance data for IDENT1 hardware and software components.

– By FOC, this data will be used to generate dashboards and reports that will be accessible through the IDENT1 intranet web site.

## 3.4 Data View

The following describes the image and data exchange formats that will be implemented for IDENT1:

**Image Storage and Compression**

– Joint Photographic Experts Group (JPEG) 6 will be used for the capture, storage and display of fingerprint and palm images. Both lossy and lossless versions will be used. JPEG is compliant with eGIF Technical Standards Catalogue V 6.0

– Joint Photographic Experts Group (JPEG) 2000 will be used for image capture from generic mark cameras.

– Wavelet Scalar Quantization (WSQ) will be used for image data exchange with Scotland during transition. After transition, images will be exchanged and stored using JPEG.

**Interconnectivity Protocols**

- Simple Mail Transfer Protocol (SMTP) will be used to communicate with various external systems including IND and Custody. SMTP is compliant with eGIF Technical Standards Catalogue V 6.0

- File Transfer Protocol (FTP) is currently used to communication between livescan units and the Central Site. This will be replaced by Simple Object Access Protocol by FOC. FTP is compliant with eGIF Technical Standards Catalogue V 6.0

**Web Services**

- Simple Object Access Protocol (SOAP) V 1.2 will be used to implement Web services between the Central Site and Livescan units, as well as to communicate fingerprint text data between the Central Site and Bureaux. It is currently implemented as an interface between Livescan and the Custody application. SOAP V 1.2 is compliant with eGIF Technical Standards Catalogue V 6.0.

**Data Structure**

- Extensible Markup Language (XML) will be used as the text data exchange format between IDENT1 and all external systems that support XML formats. It will also be used as the metadata file format for textual fingerprint information passed to COTS applications such as match engines. XML is compliant with eGIF Technical Standards Catalogue V 6.0.

- ANSI/NIST-ITL 1-2000 V 4.20 will be used as the standard format for the exchange of fingerprint text and image data with external systems. These files can be embedded within SMTP base email messages.

**Encoding**

- Multipurpose Internet Mail Extension (MIME) will be used to encode binary data for attachment to SMTP and SOAP message. MIME is compliant with eGIF Technical Standards Catalogue V 6.0.

## 3.5 Physical View

A further description of the IDENT1 solution from a hardware perspective is provided in this section.

### 3.5.1 Central Services Hardware

Figure 3.5-1, which is extracted from the Northrop Grumman proposal, shows the Central Segment Hardware architecture, indicating what hardware is used within each of the eight Central Services components. The same configuration resides at the secondary site. Standard COTS hardware is used throughout Central, employing standard, widely scalable and extremely reliable high-performance Sun (UltraSPARC technology) hardware for server functions and high-performance Appro (Intel-based or AMD-based) computers for specialised backend matching functions as KBMs and management servers.

Sun/ Hitachi RAID hardware is used to provide high-availability and recoverable data storage. The Sun StorEdge 9900 series offer extreme levels of availability, performance, and connectivity for the data center. The StorEdge 9900 series are optimized for the Solaris Operating Environment, and include proactive maintenance service with "call-home" capability and are supported by global mission-critical support centers. For a data backup solution that can grow and change with data requirements, Northrop Grumman will incorporate modular scalability utilizing Super DLT technology with the ATL M1500 tape library. For critical IDENT1 servers, a dedicated tape library backup to each server will be employed. For management servers, a backup scheme will be implemented over the network to a dedicated backup server.

To ensure system availability IDENT1 hardware has been designed to take advantage of each vendors integrated system redundancy capabilities in all hardware components and subsystems. Some examples include; servers configured with; multiple CPUs, extended memory, redundant I/O paths to critical subsystems such as dual fiber channel connections to RAID and dual gigabit Ethernet connections to the network backbone, and redundant power supplies. The central network backbone (LAN) is designed to provide dual network paths for each server.

Several different Sun servers have been chosen, based on the expected load and transaction rate. The Sun systems range from the single CPU model Sunblade 1000 workstation to the Sun Fire quad CPU V480. Each Sun server is configured with different amounts of physical memory, depending on the need determined by applications running on that server. Each Sun server runs the same version of the standard Solaris operating system.

The ***Central Administration and Monitoring*** component houses a mix of high performance dual CPU Appro computer and Sun Microsystems entry level servers such as the Sun Blade 1000 operating as a Console Management Workstation for remote "lights out management" of all Central Solaris servers, and the Sun Fire V480 as a multifunctional and auditing server. The Appro hardware provides a low cost performance based solution for management of

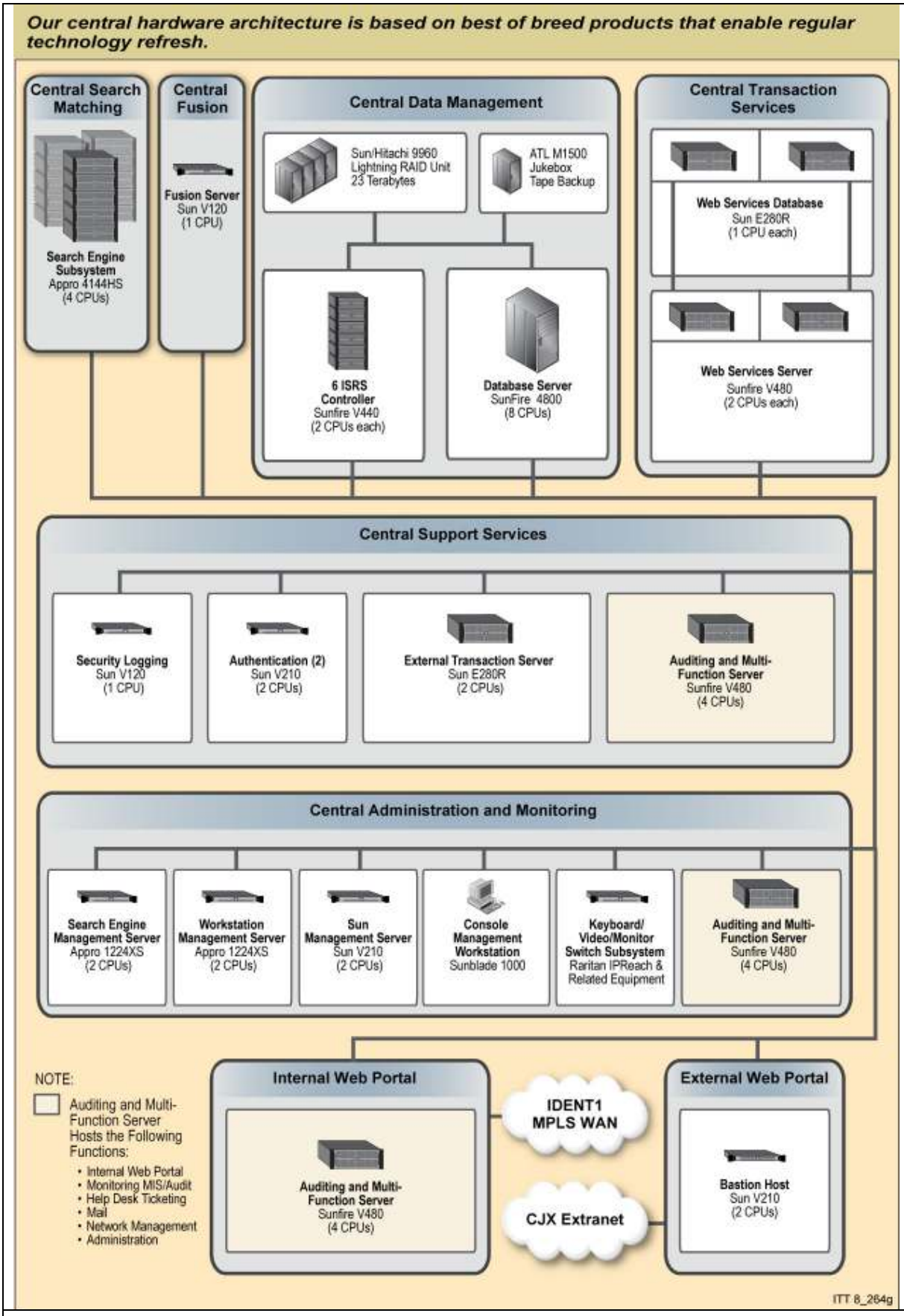



**Figure 3.5-1. Central Segment Hardware**

system wide components such as KBM search engine management, workstation management, and Sun Solaris platform management.

The ***Central Transaction Services*** component consists of two each Sun Enterprise 280R single CPU servers to support the database function for Web Services. For Web Services functionality the contractor will integrate two each dual CPU Sun Fire V480 servers will be integrated. These systems are positioned at the high-end of Sun's powerful line of rack-optimized, entry-level servers.

The ***Central Support Services*** component includes Sun servers to support system authentication and security services, logging, and External Transaction services. These systems include Sun V120 single CPU server running security logging, a Sun V210 dual CPU server for authentication services (LDAP). These systems offer high performance, reliability, and security in an ultra-dense, rack-optimized package. The contractor will also incorporate reuse with the existing Sun Enterprise 280R dual CPU server supporting external transaction functionality.

For the ***Internal/External Web Portal*** component, the contractor will integrate the Sun Fire V480 quad CPU server and Sun V210 dual CPU server. These systems provide bastion (public server access from CJX) and Web services functionality such as reporting. Again, these hardware platforms are positioned at the high end of Sun's powerful line of reliable rack-optimized, entry-level servers.

The contractor will also incorporate reuse of existing NAFIS hardware such as the Sun Fire 4800 database server for the ***Central Data Management*** component. The Sun Fire 4800 delivers Full hardware redundancy and a variety of advanced mainframe-class availability features, such as Hot CPU Upgrades and Dynamic Reconfiguration to deliver exceptional availability. This component also includes the Image Storage Retrieval Subsystem with six each, dual CPU Sun Fire V440 systems. The V440 is a high-performance, data center-class server with an extremely flexible platform for delivering low-cost, horizontally scalable services.

The ***Central Search Matching*** component is based on proven technology used on the NAFIS system. The contractor will integrate a higher performance version of this hardware for IDENT1. The Appro 4144HS has been chosen to support this function to maximize performance and lower cost by reducing the number of systems needed to meet matching requirements. The Appro computer is a quad-processor machine that uses the latest and fastest Intel or AMD processors available. The Appro runs the standard Linux operating system environment. The Appro computers chosen are identical to one another, ensuring that the KBM failover functions will operate as expected since any KBM can be substituted for another KBM to support redundancy

### 3.5.2 Bureau Services Hardware

Figure 3.5-2, which has been extracted from the Northrop Grumman proposal, depicts the hardware architecture for the bureau services and mirrors that of Central. As in Central, COTS hardware is used throughout the bureaux, employing standard, widely scalable, and extremely reliable high-performance Sun (UltraSPARC technology) hardware for server

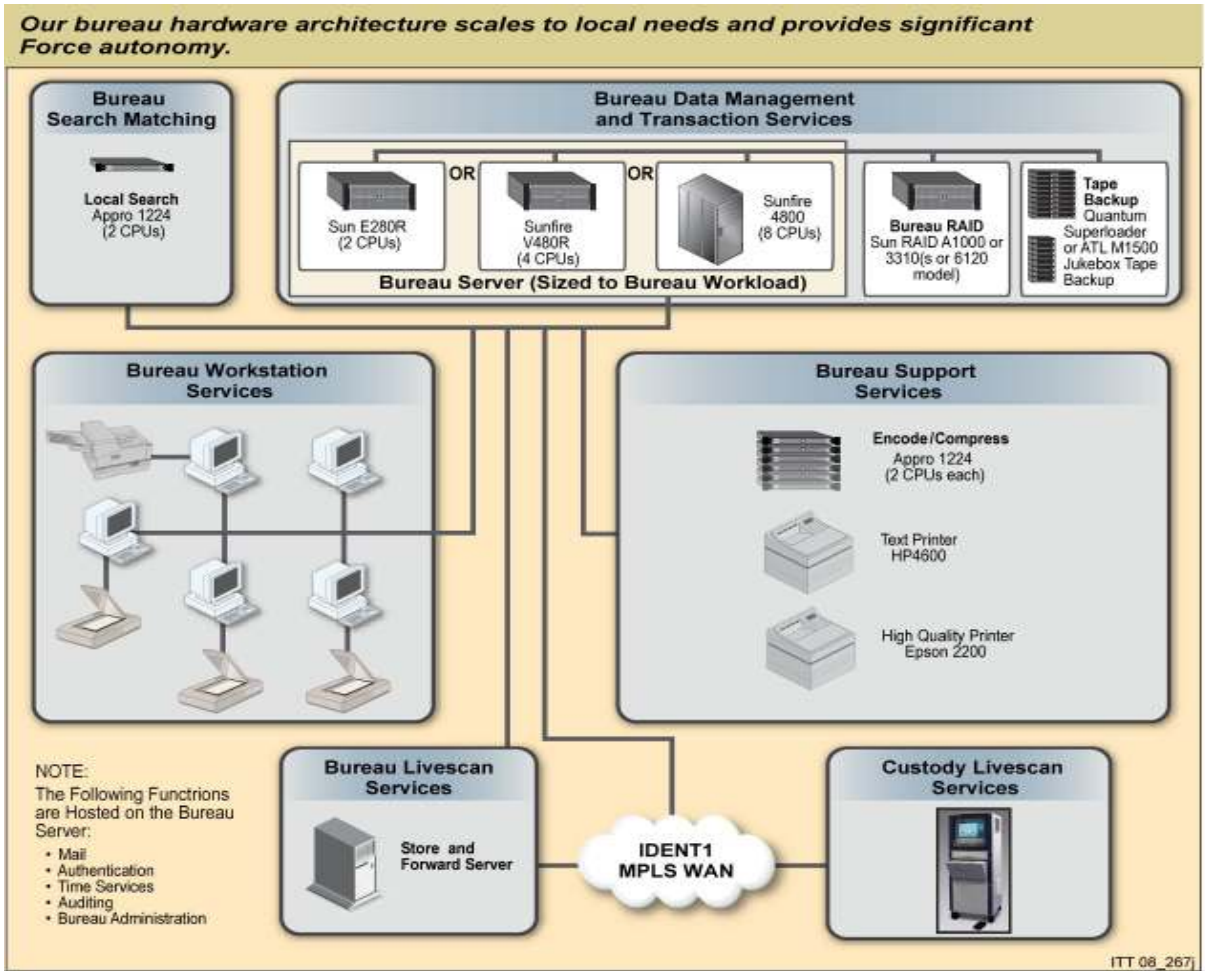



**Figure 3.5-2. Bureaux Hardware Architecture**

functions and high-performance Appro (Intel-based or AMDbased) computers for specialised back-end matching, encoding, and compression functions. The contractor will also employ Intel-based workstations to provide a fast user interface to the IDENT1 applications.

As in the Central configuration, to ensure system availability IDENT1 hardware has been designed to take advantage of each vendor's integrated system redundancy capabilities in all hardware components and subsystems. Some examples include servers configured with; multiple CPUs, extended memory, redundant I/O paths to critical subsystems such as dual SCSI interface connections to RAID, and redundant power supplies.

Since Bureaux vary greatly in size, load, and transaction rate, a "one size fits all" solution is not the right approach. Instead, different hardware profiles are developed to provide configuration options for Bureaux of different sizes. Each hardware profile consists of a set of appropriately sized hardware components that have been engineered and tested to fit the need of particular sized bureaux. Different options for Sun hardware are chosen based on the size, load, and transaction rate of a CPU, with increasing amounts of physical memory. Several different Sun servers have been chosen, based on the expected load and transaction rate. The Sun systems used include the quad CPU, Sun Fire V480 and reuse of the existing dual CPU, Sun Fire 280R, and eight CPU, Enterprise 4800 systems. Each Sun server is configured with different amounts of physical memory, depending on the need determined by bureaux workload.

A bureau profile also contains one of several models of Sun RAID devices for storage hardware used to provide high-availability and recoverable data storage. Smaller bureaux will be integrated with the reuse of existing Sun StorEdge A1000 series arrays, which provide proven hardware reliability that is currently used in the NAFIS bureaux architecture. In addition, larger bureaux will be fitted with newer technology RAID consisting of Sun StorEdge 3310 SCSI Array and Sun StorEdge 6120 Array. These devices provide a highly available, flexible, and modular storage platform that grows easily into an integrated storage system.

For a data backup solution that can grow and change with data requirements, the contractor shall incorporate modular scalability utilizing Super DLT technology with the ATL M1500 tape library or Quantum Super Loader. Each IDENT1 bureaux server will employ a dedicated tape library to facilitate system backups for complete data recovery in a disaster situation.

To support ***Bureau Search Matching*** and ***Bureau Support Services*** the contractor will employ the *reuse* of existing Appro servers. These systems are based on proven technology currently used with NAFIS system. The contractor will integrate the dual CPU Appro 1224 server to provide local search and encode/compress functionality. Although each Appro machine is configured identically, each bureau profile contains varying numbers of Appro machines, based on matching workload. This component will also include LaserJet technology based text and high-quality colour graphics printers.

To support the Bureau ***Workstation Services*** component each Bureau contains a varying number of Intel-based Workstations. Each Workstation is configured identically, which minimizes maintenance complexity. These Services provide the user with a fast user interface that includes NAFIS functionality. Workstations will be physically located at Bureau sites and communicate with the Bureau servers through Bureau LAN switches. There will be multiple workstations connected to a single bureau server. Devices to support capturing images, printing, and reading Case bar codes, will be attach to various workstations.

The quantities of mark and ten-print scanners, printers (text, graphics, barcode, and high quality), and barcode readers are determined by bureau workloads as contained in the DOR and by the number of workstations. It is recognised that changes in bureau workload, business processes, personnel, or space availability and layout may require additional resources above those initially allocated. If bureaux desire additional peripherals above the agreed-upon total, the items may be procured through the Options Catalogue.

Table 3.5-1 presents the maximum number peripherals to be installed under the contract. The actual quantity of each peripheral to be installed will be determined during the site surveys and through discussions with each bureau up to the totals shown in the table.

**Table 3.5-1. Peripherals to be Installed Under the Contract**

| Peripheral | Quantity (max proposed) |
|---|---|
| Ten Print Scanner | 54 |
| Mark Scanner | 200 |
| Barcode Reader | 210 |
| Barcode Printer | 210 |
| Text Printer | 90 |
| Graphics Printer | 90 |

| Peripheral | Quantity (max proposed) |
|---|---|
| High-Quality Printer | 90 |

At least one ten print scanner will be installed at each bureau. Each ten print scanner is directly connected to a workstation but can be moved to another. Moreover, the ten print scanner is attached to a workstation shared centrally within each bureau and, based on the flexibility of workflow, scanned data can be accessed from any other workstation on the network. Larger Bureaux will receive more ten print scanners based on throughput requirements.

Mark scanners are also directly connected to a workstation and can be moved among workstations. Moreover, based on the flexibility of workflow, scanned mark data can be accessed from any other workstation on the network. At least a single mark scanner will be provided at each Bureau. The size of the bureau (i.e., number of workstations) determines the number of additional scanners to be provided.

Barcode readers are connected via the keyboard input and, therefore, not networked. The barcode readers can be easily moved among workstations, allowing sharing of the functionality provided. At least two will be furnished per bureau. The size of the bureau (i.e., number of workstations) determines the number of additional readers to be provided.

Barcode printers are not networked and are required to be near at hand for ten print processing. At least two will be furnished per bureau. The size of the bureau (i.e., number of workstations) determines the number of additional readers to be provided.

Text, graphics, and high-quality printers are shared, networked resources. For this proposal, the current printer/workstation ratio is scaled to the projected number of workstations. At least a single network printer of each type will be provided at each Bureau. The size of the bureau (i.e., number of workstations) determines the number of additional printers (up to five of each will be provided).

As described in Central Services Hardware, the use of standard, consistent hardware components provides the best value for the customer by reducing maintenance costs and providing the maximum amount of flexibility for vendor choice and upgrade options.