

Attachment B-1
Description
Contract Change Note 050
IDENT1-LANTERN Service Expansion

Table of Contents

1. Purpose 2

2. Scope..... 2

 2.1 Architecture 3

 2.2 Approach..... 5

 2.2.1 Transition 6

 2.2.2 PNC Warning Flags 7

 2.2.3 User Authentication 8

 2.2.4 Service Level Requirements (SLR) 10

 2.3 Pricing Structure 11

3. Component Provision 12

 3.1 Mobile Fingerprint Readers (MFRs) 12

 3.2 Secure Infrastructure 13

 3.3 Data Connectivity 15

 3.3.1 Mobility Expansion 15

 3.3.2 Subscriber Information Modules (SIM) 16

4. Deliverables 16

 4.1 Non-Document Deliverables 16

 4.2 Document Deliverables 17

5. Authority’s Responsibilities 18

 5.1 Customer Furnished Equipment (CFE)/Customer Furnished Information (CFI)..... 18

 5.2 Schedule O (Documentation Requirements) Document Review and Approval..... 18

6. LANTERN Stakeholders and Responsibilities..... 18

7. Schedule..... 19

8. Options..... 19

9. Assumptions and Conditions 19

Attachment B-1

Description: IDENT1-LANTERN Service Expansion

1. Purpose

This revised proposal provides the price for the deployment and support of IDENT1-LANTERN Service Expansion including new requirements added in March 2008. It follows from the successful LANTERN pilot, which has been in operation since November 2006.

The purpose and overarching objective of the LANTERN project is to provide police with portable fingerprint capture and results from searching the Unified National Collection via a secure wireless link. It features:

- Efficient capture of fingerprint details suitable for identifying individuals in an operational environment;
- Real-time searching of the unified fingerprint collection held on IDENT1 with timely responses on matched subjects containing information to aid officers in their decision making process.

CCN014R2 “LANTERN Pilot Phase 2 – Implementation Phase” and the follow-on extension of service CCN014R2A proved the viability of the LANTERN Concept of Operations, including its operational human-computer interface and the interface with Central facilities housing the unified fingerprint collection. It validated the technical approach and business case for LANTERN through the use of ten (10) pilot Forces equipped with one hundred (100) hand-held Mobile Fingerprint Readers (MFR) to assess workload implications for the fingerprint matching capacity.

Based on user feedback concerning usability of the solution and validation of the business process model, and on the fingerprint matching capacity requirements for a larger operational deployment of LANTERN, an expansion of the scale of the pilot was exercised and is being implemented under CCN040. It doubles the number of MFRs to two hundred (200), and deploys them to an additional ten Forces for a total of twenty (20).

2. Scope

This description indicates the scope of expanded services covered by the proposed price for CCN050. It describes an expansion of LANTERN service to a greater number of police forces throughout England and Wales, making fingerprint identification readily available to more officers in the pursuit of their duties. This involves procurement of additional MFRs, with spares and warranty service, and implementation of customised MFR software designed to meet requirements unique to LANTERN. It also requires expansion of the Central facilities where fingerprint data is maintained and searches are performed. Higher capacity computational resources will be implemented to process a larger workload of searches. Refinement of the detailed design, development, integration, and implementation services will be provided for the expansion, including deployment and support for the added MFRs. The requirements set¹ provided by the Authority for the IDENT1-LANTERN Service Expansion has been annotated with responses to each requirement. It is attached as Annex 2.

The features required for LANTERN operation have been previously developed under the aforementioned pilot (CCN014R2). The proposed IDENT1-LANTERN Service Expansion makes full use of the existing baseline of capabilities, refining them to ensure robust operation on a larger scale, and expanding their use to a larger user community. In response to newly defined requirements, this proposal adds the following features:

- User-level authentication upgrades the security solution from device-based authentication, as delivered in the pilot, to user-level authentication, where all users have unique and authenticated identities that follow them to any MFR to which they are assigned.
- PNC Warning Flags displayed on the MFR augment the current data on respondents from LANTERN searches. Display of PNC Warning Flags to LANTERN users, just as demographics have been displayed in

¹ LANTERN CCN050 Requirements v0_1 draft.doc dated 20 March 2008

the LANTERN Pilot, adds another dimension of valuable and timely information to aid in police decision making.

- Service Level Requirements (SLRs) are proposed for major performance and technical support areas along with the additional metrics reporting and analysis to determine and report them.

In order to meet the expected workload increase from MFR deployment to a larger number of users, the centralised capacity to perform fingerprint searches and return useful and timely responses to LANTERN-equipped officers is also increased through the addition of search engines and associated kit. The search engines are comprised of matchers using specialised algorithms similar to others used in IDENT1 but tailored to optimise them for the unique plain-to-roll two-index-finger searches of LANTERN.

Software hosted on servers manages the search/match functions, performs fingerprint feature extraction, and provides a web-based interface through which the mobile devices communicate with the Central facilities. Two Central facilities each provide similar functions, enabling sharing of search load and continuity of operation in case of planned or unplanned interruptions in service at one of the sites.

The LANTERN fingerprint matching resources and associated servers are dedicated to LANTERN operations, so search performance is not subject to variations due to workload of other search services.

The Central architecture is modular, so the capacity can be augmented as MFRs are added or if workload rises for other reasons. This proposal presents price points for 1,500 and 2,500 added MFRs and the corresponding Central services provided as needed for the MFR quantity.

2.1 Architecture

The IDENT1-LANTERN Service Expansion architecture is depicted at a high level in Figure 2-1.

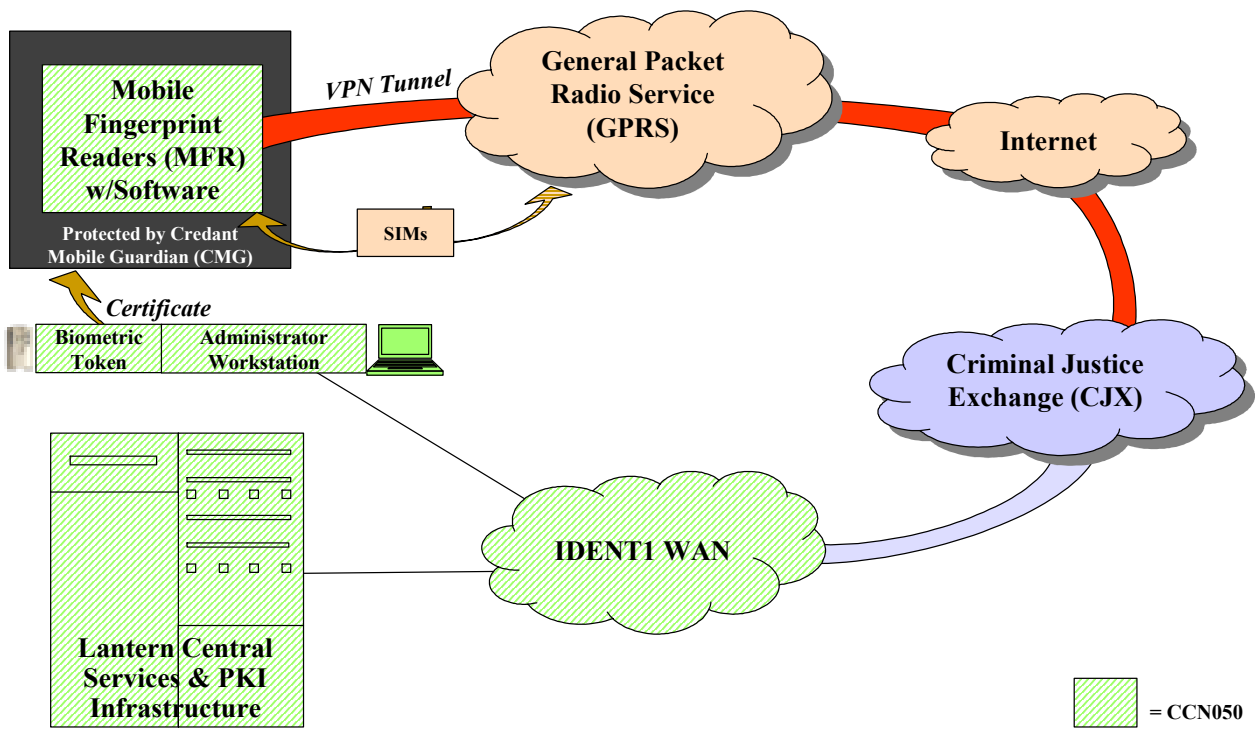


Figure 2-1 IDENT1-LANTERN Service Expansion – High Level Architecture

The MFR uses updated Credant Mobile Guardian (CMG) client software as proven in the Secure Remote Access Solution (SRAS) to protect the data at rest, and virtual private network (VPN) software to protect the data in transit. The MFR is paired with a biometric token that enables user authentication as a prerequisite for opening a VPN session with Central. A device-level PIN is used for administrative access for configuration or repair.

Transmissions are carried over GPRS communications provided under existing carriers used by each Force. LANTERN operates with all of the four leading carriers used by Forces. The IDENT1-LANTERN Service Expansion also provides mobility expansion to make the best use of communications links for secure messaging to/from the MFR. Mobility features from Brand Communications replace the Aventail client used in the pilot, enabling MFRs and even individual sessions and transmissions to utilise a choice or even a combination of networks to ensure the highest quality link available. It will also allow for future addition of new networks such as WiFi that offer faster or fuller coverage than GPRS.

Messages from an authenticated user are passed securely via a VPN tunnel through the GPRS network and over the Internet to a VPN concentrator. The user certificate validity is checked against a certificate authority accessing a certificate revocation list (CRL). The VPN tunnel ends at the concentrator located in the IDENT1 DMZ, which then passes the message securely to the LANTERN Central via the IDENT1 LANTERN gateway. There, the LANTERN Central facility processes it, performs the requested fingerprint search, and returns a response via the same path.

The infrastructure for managing user certificates, assignments and software updates will be centralised with distributed components at the force levels to support activities of enrolment and device management.

Authentication, authorization, and accounting at the individual Lantern user level are provided by four subsystems: a Public Key Infrastructure (PKI), user credential device management, endpoint security device management, and increased security protection and logging capability. Specifically:

- Entrust PKI provides the infrastructure to provision and manage X.509 Version 3 user certificates to 12,000 users. The PKI is scalable and can manage more than 100,000 users simply by the addition of more user licenses. One hundred (100) Administrator Workstations are provided at force locations that have IDENT WAN connections (e.g., for existing Livescan). These are used for local management of user accounts, certificates and credential storage devices.
- Privaris plusID biometric tokens are used to securely store the individual user certificates and to authenticate the user to the MFR, the VPN endpoint, and to the IDENT1 Lantern search service. Each Lantern user carries his or her own token, and uses it to authenticate the user to the MFR, so it can in turn identify the user to the Lantern services. The Administrator Workstations are also used to manage the plusID devices.
- Sun Identity Manager, already in use for provisioning and management of IDENT1 user accounts, is expanded to Lantern users as well. Identity Manager functions are integrated with the Entrust and Privaris management tools to provide a single interface for user account, certificate, and device management. User accounts can be managed by Force personnel, to include creation, modification, and deactivation of user accounts, revocation of certificates, and token assignment/configuration.
- Credant Mobile Guardian Enterprise Edition provides endpoint security for the MFRs. The Administrator Workstations are used to manage the MFRs via a new CMG infrastructure contained within IDENT1.

The IDENT1 security architecture is enhanced to include additional protection of the Lantern servers, the CJX-facing firewalls and DMZs, as well as providing additional logging of all affected interfaces.

This proposal provides for LANTERN fingerprint identification services to be provided from a variable number of hand-held MFRs rolled out to Police Forces without restrictions on quantities per Force. Deployment distribution can be defined according to Force needs.

The MFRs previously provided under the pilot will continue in service under the terms of their existing contract (CCN014R2A or CCN040). They are not covered by CCN050.

The rate of deployment will be raised from the current 20 MFRs per week at 2 Forces to meet the greater volumes of the IDENT1-LANTERN Service Expansion. Using the current resources and procedures as a baseline, staff allocations and multiple shifts will be combined with procedure improvements that raise productivity to sustain MFR build and deployment at a rate of 100 per week. It is a key objective to deploy to the Forces as fast as practicable so the value of LANTERN begins to accrue as soon as possible. Specific scheduling of deployments to each Force will be subject to agreement with the Authority and the Forces.

The IDENT1-LANTERN Service Expansion adds to the dedicated LANTERN matching subsystem residing on the IDENT1 SISP. Its database is updated from the IDENT1 database to keep it current as changes are made to the Unified National Collection. The matching subsystem provides print-to-print searches of index fingers against composite prints in the database. It is not required to search multiple registrations, nor fingers other than index fingers (numbers 2 and 7).

Central search capacity and matching response times are summarised in the LANTERN Performance and Scalability Report (CCN014R2-20.2-1.0). The capacity is based on analysis of usage statistics collected during the LANTERN Pilot Phase 2 - Implementation Phase. The report predicts matcher capacity needed as a function of the number of deployed MFRs, in a way that reduces procurement costs. The predicted capacity is substantially less than would be needed for an unlikely worst case in which every MFR submitted a search at exactly the same time, and is also about 2/3 less than would result from simply scaling up the pilot MFRs and matchers proportionally. However, it is greater than the capacity required to only keep pace with an invariant search request rate during each hour. Because of the 5 minute response time requirement, it must allow for limiting queues to short lengths to permit fast response times in the face of any reasonable expectation of peak loads. That is the basis of the proposed matcher complement. Imposition of an SLR on response time with a more stringent target than on the pilot will require additional resources.

Service including implementation, deployment and operation of the MFRs, Central facilities, and associated security/user authentication is included for a period of three (3) years from CCN050 approval. Indicative pricing for support services is provided for two optional one-year extensions beyond the period of performance. Technical refresh of MFRs will be provided through the change control process upon the Authority's request.

2.2 Approach

The general approach of the IDENT1-LANTERN Service Expansion is in five (5) strands:

1. Customisation of the third generation SAGEM RapID to meet LANTERN MFR requirements
2. Refinement of the existing functionality of the Central software and its interface to the MFR
3. Boosting centralised search capacity to handle a higher search rate from more MFRs
4. Implementing user-level authentication and a PKI infrastructure integrated with IDENT1 identity management and associated certificate/security management
5. Strengthening of the process infrastructure providing build and support services as well as added metrics needed for reporting SLR achievement.

The approach is shown in Figure 2-2. It shows an Incremental CDR, which covers all changes to the pilot design. The changes in design and processes are to provide a more robust LANTERN infrastructure commensurate with the larger scale of operations. The IDENT1-LANTERN Service Expansion does not propose changes in design to add new search functions, but rather to strengthen the implementation of existing LANTERN functions. Integration of the MFR with the communications and security infrastructure takes place in the UK, while MFR/Central integration and test takes place in parallel in the US. The MFR functionality, Central interface and Central search functionality is proven through factory test in the IDENT1 Fairfax facility without integrated client communications and security installed. Then the integration and test is completed with fully integrated security functions and communications with LANTERN central in the UK.

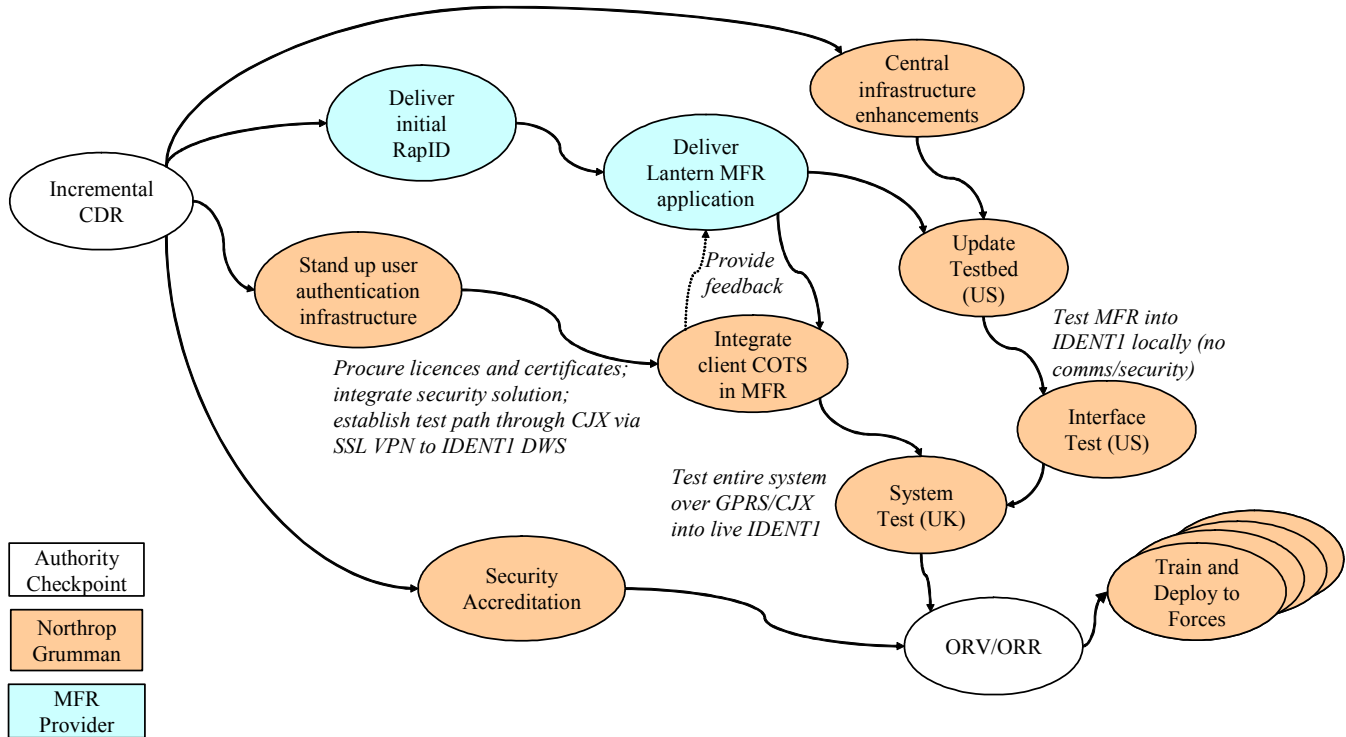


Figure 2-2 LANTERN Implementation Approach

Northrop Grumman tests all the LANTERN functions including the communications and security infrastructure. The security infrastructure for user authentication is also subject to accreditation by the Authority prior to deployment of MFRs, and this as well as successful test completion are prerequisites for the Operational Readiness Review (ORR). The system test runs against the production IDENT1 data on the LANTERN KBMs seeded with a few individuals to allow testing using searches returning respondents and those with no respondents. At the completion of the system test and subsequent review, the phased rollout will commence as set out in a schedule to be agreed. The Fairfax test bed will be updated to reflect the operational configuration.

2.2.1 Transition

The high-level schedule is shown in Schedule Attachment B-2, “Proposed High Level Schedule.” The significant features are deployment of up to 1,500 MFRs by 11 months after CCN approval (MAC) or 31 March 2009 assuming a CCN050 start date by 1 May 2008. Deployment is planned to start 16 weeks prior to that, making allowance for a one-week hiatus during the Christmas holidays.

Sagem can deliver up to 150 MFRs per week from their factory, which provides a margin over the planned 100 per week deployment rate. MFRs are delivered by Sagem directly to the point of build at the Hendon Data Centre, where subcontractor Phoenix loads the software image onto each MFR and performs any device-specific configuration. From there, the MFRs are shipped directly to the force(s) next in line for deployment according to the NPIA-defined sequence. They arrive at the Force in time to be unpacked, checked out and ready for use in training of users and Force IT, and then the scheduled go-live.

The search-match facilities at Central continue in operation processing searches from the 200 previously deployed Pilot MFRs as long as their service continues. This is covered under Pilot CCNs (CCN014R2A and CCN040) through 12 December 2008. Installation of the kit to add Central searching capacity will be during planned downtimes, and have minimal effect on ongoing LANTERN operations.

Service support for the MFRs from the Pilot is also covered under Pilot CCNs through 12 December 2008. We will work with the Authority to schedule deployments of the new MFRs by force in accordance with police priorities. For example, at the Authority’s discretion, MFRs from the pilot could be replaced by new ones at the pilot forces on the earliest deployments if desired to provide these established users with the expanded

capabilities first. This would also minimise the overlap period when multiple generations of MFR were in simultaneous operation. Once the old MFRs are phased out, training and documentation would only need to follow one track, service desk troubleshooting operations would be simpler, and sparing would not have to account for MFR type so swapping would always be of an identical type. However, this would reduce the cumulative Lantern deployment count from 1700 to 1500.

An alternate approach would be to extend the Pilot via Change Control to cover its 200 MFRs beyond 12 December 2008, and concentrate them at selected forces, supported with spares from the Pilot; then deploy only new MFRs to all the other forces. This approach would result in old and new MFR operation overlapping for a longer period.

In any event, because of the possibility of overlapping operation with MFRs that are not a part of the IDENT1-LANTERN Service Expansion, backward compatibility considerations have been addressed in this proposal. Pilot MFRs can continue to operate in accordance with Pilot requirements even after updated software is installed at Central under the IDENT1-LANTERN Service Expansion. They are not to be retrofitted under this CCN to add new functionality, but will continue their operational capability using device-level rather than user-level authentication, and not displaying any PNC warning flags. There is no intention to modify pilot MFRs to run the updated software of the IDENT1-LANTERN Service Expansion, as this would be complicated due to the different operating systems they use. If there is a period of overlap, Service Level Requirements on Central Availability, search volume, and response time will not distinguish searches from old vs. new MFRs.

2.2.2 PNC Warning Flags

The IDENT1-LANTERN Service Expansion provides functionality to display PNC Warning Flags² to the user on the MFR screen. The proposed functionality builds upon existing IDENT1 functionality that provides this data to Livescan operators and is implemented by a simple extension to the existing Lantern interface.

These data fall within three classes:

- Warning Signals
- Information markers (data item no. 014 in the Data Definitions)
- Wanted/Missing (data item no. 302 in the Data Definitions)

In the first two classes, data are displayed as a sequence of valid two-character codes separated by spaces. In the third case, a single text string of up to eight characters is displayed, being one of a constrained list of valid values. For example:

```
WS: FI MN AG
IM: SO HA
WM: LOCATE
```

These lines are only displayed when search results identify a respondent for whom IDENT1 holds PNC Warning Flag information. If there is no PNC Warning Flag data for the respondent, the MFR will display the usual data including CRO, name, date of birth and sex. In the case where PNC Warning Flag data cannot be retrieved for insertion into the search results, the MFR will display a string such as "Not Available" as LANTERN currently does for search results demographics.

LANTERN obtains the PNC Warning Flags from the IDENT1 AFR Server when a respondent's fingerprints are matched. This is the same process as developed in the Pilot for demographic data. The implementation is dependent upon Back Record Conversion (BRC) being complete. It is assumed that

² PNC Warnings data is defined in Phoenix System Data Definitions – Version 3.41 – March 2007

the PNC side of the interface has been developed and commissioned, and that BRC of the PNC WN data has been completed before this capability is deployed.

The current LANTERN Interface Control Document (ICD) will be extended to allow incorporation of this new data. Three user-defined fields in the NIST Type-2 record will be added to carry warnings data, which will be formatted by the server. The MFR will simply display what the server sends in these new fields without modification.

All warnings data sent to the MFR will be recorded at Central as audit information. This will include as a minimum:

- Date/time stamp
- User ID
- CRO No
- Warning Signals, Information Markers, Wanted/Missing flag

Audit information will not be included within scheduled reports. It will be available by request to the IDENT1 Service Desk from persons authorised to have access to it.

This CCN makes no allowance for retrofitting this functionality to Pilot (CCN014 and CCN040) MFRs. If required, this functionality can be included within a future CCN to extend the life of these devices. Note that this CCN would also have to include user-level authentication to allow PNC data to be available to the Pilot MFRs.

2.2.3 User Authentication

User authentication for Lantern is via X.509 Version 3 certificates assigned to each user. The certificates are used for authentication to the MFR, the VPN server, and the IDENT1 Lantern service. The certificates are loaded on a biometric token assigned to each user. The bio-token is a pocket-sized device built by Privaris that uses a solid-state fingerprint sensor and an internal matching engine to match a user's fingerprint and unlock the certificate.

The most important feature of this approach is that a user need only authenticate once per session, and is not required to remember a PIN or go through a large number of steps to logon to the Lantern service. The use of fingerprint verification to gain access to LANTERN services via the bio-token also provides a higher level of security than PIN authentication. Also, LANTERN services can be provided based on a user's role rather than simply to anyone using the MFR. This makes it possible to deliver the necessary information only to the officer with a need-to-know.

The bio-token connects to the MFR wirelessly via a secured Bluetooth path, and authenticates the user to the MFR using standard Microsoft Windows cryptographic protocols. A copy of the certificate is then uploaded to the MFR for use until the unit is turned off or the user logs off the device.

The certificate copy is then used to authenticate the user to the VPN access point as well as the IDENT1 LANTERN service. For the VPN, the certificate is used by the client application on the MFR for authentication. This is in contrast from the current device-based VPN authentication, which allows the MFR to connect to the CJX without identification of the user connecting.

For the LANTERN application, the authentication occurs via a proxy application on the MFR. The use of the proxy application removes any dependency on the Sagem proprietary application on the MFR and uses standard protocols to authenticate the user to the IDENT1 service for both search requests and

result requests. The DMZ Web Server (DWS) hosting the Lantern service interacts with the proxy to validate the authentication and render the service requested.

All auditing of network access and search or results requests and responses will be by user, allowing full accountability of the service usage.

The enrolment and provisioning of users is performed via the IDENT1 Sun Identity Manager. The web-based application allows a user to be added as an IDENT1 user with the appropriate Lantern roles. If the user is already enrolled in IDENT1, an additional role can be added to his profile.

The assignment of the Lantern role to a user will initiate a workflow to create an X.509 certificate, and notify the user's force-level administrator that a new user must be processed. The administrator then meets with the user, assigns a bio-token to the user, personalises the bio-token to the user, and loads the certificate. One-on-one training for use of the bio-token can also be done at this time.

Administration of the PKI infrastructure with 12,000 users requires a carefully conceived plan for making the needed capabilities available at the force level. A PC-based Administrator Workstation is provided at each MFR-equipped Force. It allows daily activities connected with user authentication functions of user, bio-token, and MFR administration to be performed locally. These include police (Force IT) activities of:

- Setting up bio-tokens and MFRs for assigned Force officers
- Enrolment of new users via communication with Central
- Revocation of users no longer authorised for LANTERN use via communication with Central
- Level 1 resolution of trouble calls that require only refresh of the MFR software load
- Loading software updates obtained from Central (can be done while charging)
- Ensuring MFRs are charged when not in use
- Physical control of MFRs or bio-tokens, and tracking checkouts by users.

This capability is provided by 100 Administrator Workstations located at the force-level with existing links to the IDENT1 WAN link as currently used for Livescan. As shown in Figure 2-3, the link is used for communicating to the Central PKI and other management assets. The use of the Administrator Workstations is detailed below.

- The Privaris plusID Manager application running at the Administrator Workstation is used to manage the plusID bio-tokens. It updates the device firmware, personalises the device to a user and tracks the assignment of the devices to users. As for Credant Mobile Guardian (CMG), a central server manages the devices from one location.
- Once a user has been assigned a bio-token, he can use any MFR. As with any Bluetooth device, the bio-token must be paired to the MFR prior to use. This is a simple process using Privaris plusID Manager to pair the user's bio-token to a specific MFR. Up to four specified MFRs may be paired to each bio-token at any given time. The Privaris plusID Manager application can be used to delete an existing paired device or add a new one.
- The workstation is also used to maintain the MFRs via CMG. The MFRs will be hot-synced as necessary to the workstation for centralised management of the software configuration on the MFR or to restore an MFR to a known factory-fresh state. The provision of this management software separately from that used for the pilot affords better asset tracking and management and reduces the repair duration for devices that only need refreshing.

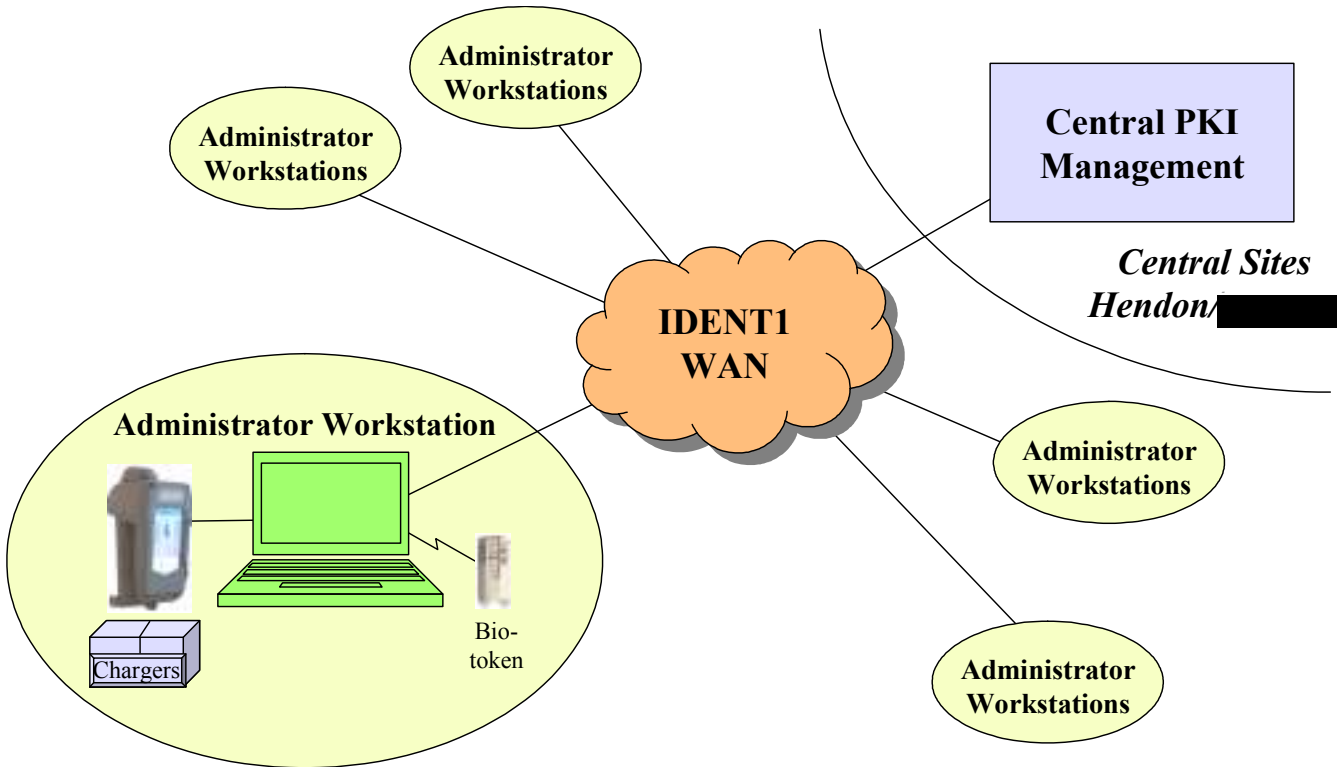


Figure 2-3 Administrator Workstations for Administering User-Authenticated Security

2.2.4 Service Level Requirements (SLR)

The Authority has provided an SLR framework (Service Level Reporting / Agreement Requirements Framework) as the basis for CCN050. Northrop Grumman has used this document for the basis of our proposal, with the caveats noted in this section, and in an annotated version of the document included as Annex 1.

As the support to the Lantern pilot to date has been performed on a best endeavours basis, rather than under a formal SLR reporting and financial framework, this proposal includes all the initial effort to set up the expanded data gathering/analysis/reporting at the outset, and ongoing effort to perform the data gathering/analysis/reporting including liaison with the Authority. These efforts include:

- New and expanded service level metrics (availability, response time, volume, problem management, matcher quality assurance test)
- Increased data gathering/analysis/reporting on service level metrics to score SLR compliance
- Formal monthly SLR Report
- Monitoring/reporting of technical support service management
- Additional Service Desk staff to provide full coverage 24/7 to address the nearly 10-fold expansion in LANTERN MFR, and 12,000 simultaneous users
- Service manager assigned to LANTERN
- Point of contact for daily/weekly interface with NPJA
- Monitoring current status of tickets
- Setting up service assurance methodology for LANTERN-specific tracking building on the IDENT1 infrastructure

Only calls, incidents and problems relating to LANTERN will be covered by these SLRs. Other services that use central facilities and/or share the Service Desk such as IDENT1 Livescan, UK Visas, etc. are covered by their own metrics and shall not impact scoring of LANTERN service level metrics.

Service Level Requirements on Central Availability, search volume, and response time will not distinguish searches from Pilot vs. new MFRs. Technical support SLRs for incident and problem resolution and service requests on pilot MFRs are excluded from CCN50 SLRs and remain on reasonable endeavours basis in accordance with their respective contracts (CCN014R2A or CCN040). All calls to the Service Desk will be included in the totals, but if a resolution target for an incident or problem for a Pilot MFR is exceeded, it isn't counted against the score. Any training requests or new equipment requests relating to pilot MFR's are excluded from the SLR.

The Service Management will be provided from the existing IDENT1 Service Delivery organization, with enhancements and modifications to meet the specific Lantern requirements. Whilst the basic reporting elements and identification services are consistent with existing IDENT1 services, the significant increase in devices, deployment, users and concept of operation, to include the new User Level Authentication, requires a significant uplift.

Basic Service Desk functionality will be provided from existing IDENT1 facilities, with split site operation continuing for disaster recovery and continuity of service considerations. Therefore, basic facilities and infrastructure costs are already provided under IDENT1. Personnel and programme management resources will also continue within the IDENT1 organization structure, to further limit costs to the LANTERN programme. As an inclusive element of IDENT1, 2nd, and 3rd level support will continue to be augmented by Northrop Grumman's IDENT1 engineering and development resources both in the US and UK.

It is anticipated that while existing structures, processes and procedures will form the basis of support for the IDENT1-LANTERN Service Expansion, dedicated resources will need to be provided to address the unique aspects of this service. The User Authentication, to include certificates, tokens, log-ons, privileges, and the sheer number of deployed devices will necessitate dedicated resources. We have proposed an increase in staff, particularly during the early phases of deployment and implementation, with augmentation by existing IDENT1 staff for off-hours or peak demand periods. Likewise, we envisage dedicated service management staff to work with the Authority and user community on the standup of the service, as well as tracking and reporting a separate set of metrics. Additionally, the number of devices, deployed in a mobile application, necessitates a significantly more detailed logistics model to track devices during operations, as well as the repair and maintenance cycles.

As the IDENT1-LANTERN Service Expansion also has new LANTERN requirements, such as for PNC Warning Flags, and for capabilities for capture and display of photos, it is anticipated that additional changes to Remedy will be required to stay current with the operational deployment, but will likely add increasing call volumes, particularly to the "Service Request" category. While it is recognized that the SLA weighting to this area is small, the labour to operate the Service Desk and to track and report on this category, by force, will be a significant increase to current IDENT1 requirements.

2.3 Pricing Structure

Northrop Grumman has designed its commercial offer to the Authority to enable them to tailor the procurement to fit an undisclosed budget based on either 1,500 or 2,500 MFRs, both with accommodation for up to 12,000 simultaneous users. The approach segmented the fixed cost (not dependant on quantity) and variable costs (dependent on the quantity of MFRs and service). This is a logical approach because the costs of the MFRs and of the corresponding matchers to process their search volume represent a major share of the total cost.

Fixed costs include non-recurring and recurring costs incurred for project activities regardless of MFR quantity and provide for technical engineering, development, and program management to support the IDENT1-LANTERN Service Expansion over the CCN050 term. The majority of these fixed costs will be expensed in the first year to move the LANTERN capability from a Pilot to an operational service delivery. The fixed costs cover development of refinements to the existing LANTERN functionality, and first-article verification activities of integration and test. Fixed costs also cover the implementation of a more robust project infrastructure suitable to support the expanded scale of operations of the IDENT1-LANTERN Service Expansion, especially the new requirements of user authentication and SLRs.

Variable costs include a wide range of costs incurred per the incremental deployment of the MFR quantities. Variable costs include not only the MFR itself, but also the Central upgrades along with the matchers (KBM kit and software licences) needed to process the higher search volumes expected from the larger number of MFRs, and the associated labour to prepare and support the deployed MFRs.

The unit cost per MFR is lower at higher quantities due to economies of scale, wider amortisation of fixed costs, and progressive discounts from our suppliers.

Some non-recurring activities are necessary to move beyond the waivers and compromises that were accepted for the pilot, and into a more expanded and extended deployment. These include changes to accommodate the larger number of users with certificates and authentication devices, extension of load balancing to use resources most efficiently, resolution of operational issues that were identified during pilot usage, and consolidation of LANTERN metrics to enable more effective use even with increases in data size and demands for its use. A mix of fixed and variable costs cover activities to continue and strengthen the services provided to ensure successful LANTERN operations including Service Desk incident response and management, as well as trouble ticket escalation needed to resolve problems. Deployment of new MFRs is supported by integration, testing, build, installation and commissioning of MFRs and Central resources.

To keep training and service economical in the face of an enlarging scale of operations, we have included development of computer-based training (CBT), which can be replicated inexpensively on CD for the growing number of Force IT and trainer personnel, and an enhanced distributed support model to handle the scale of the larger and more dispersed complement of MFRs.

The approach has been planned for compatibility with future implementations that may be dictated by even larger deployments, added functionality or extended period of service. These include such activities as:

- Source selection and certification of multiple MFR types
- Supplanting of GPRS as the wireless link for LANTERN
- Central facility upgrades of space, power and HVAC
- Extension of service period beyond the proposed period of performance
- Technical refresh of the MFRs
- Implementation of new desirable LANTERN functions such as photo capture or GPS geo-location.

Because of the complexity and number of issues that require further discussions between Northrop Grumman and the Authority, these are not priced at this time.

The costing is based on a CCN050 start date of 1 May 2008, and a period of performance of 3 years concluding on 31 April 2011. Indicative pricing is provided for one-year extensions. Services from the full MFR quantity desired must be ordered at the outset in order to allow the economies on which the pricing is based.

3. Component Provision

3.1 Mobile Fingerprint Readers (MFRs)

Mobile Fingerprint Readers (MFRs) from SAGEM Sécurité (SAGEM) have been used in the LANTERN pilot. The first-generation MR100 was criticised for losing its software load when the battery was allowed to run flat by

failure to recharge it promptly. The second-generation MR100b solved that problem by storing software in a non-volatile memory. The third-generation MR1100g is offered for the IDENT1-LANTERN Service Expansion. It also uses non-volatile memory, and adds an industrial grade PDA computer to the handheld unit. It uses a modem that is integral to the PDA rather than an external peripheral. This measure will avoid problems of compatibility between the modem and the operating system. It also has a camera, which opens future opportunities for operational benefits such as local facial image capture to link subjects to searches, transmission of photos from LANTERN to Central facilities for further uses such as facial recognition or sharing with a facial image database (e.g., FIND).

An alternate MFR source, Cross Match Technologies, Inc. (Cross Match), was evaluated during CCN009 "LANTERN Pilot Phase 2 - Specification Phase". It was offered as an option under CCN014R2, but was not exercised by the Authority.

A plan for certification of multiple MFRs has been discussed with the Authority, but is not proposed for this phase of LANTERN. Northrop Grumman offers to discuss with the Authority its role in this important endeavour. We believe that development of multiple MFR sources can result in risk reduction and substantial cost savings, especially at large MFR quantities, because it will improve procurement stability and encourage price competition. The non-recurring cost for this is not included in the price for the IDENT1-LANTERN Service Expansion.

3.2 Secure Infrastructure

One of the Authority's challenges in providing mobile identification has been the incorporation of a security infrastructure providing authentication and a secure communications path for the mobile environment. A secure infrastructure is required for police mobile communications and is not limited to LANTERN. The requirement for user-level authentication for the IDENT1-LANTERN Service Expansion adds a number of new components to the architecture for user and MFR management. They are shown in Figure 3-1.

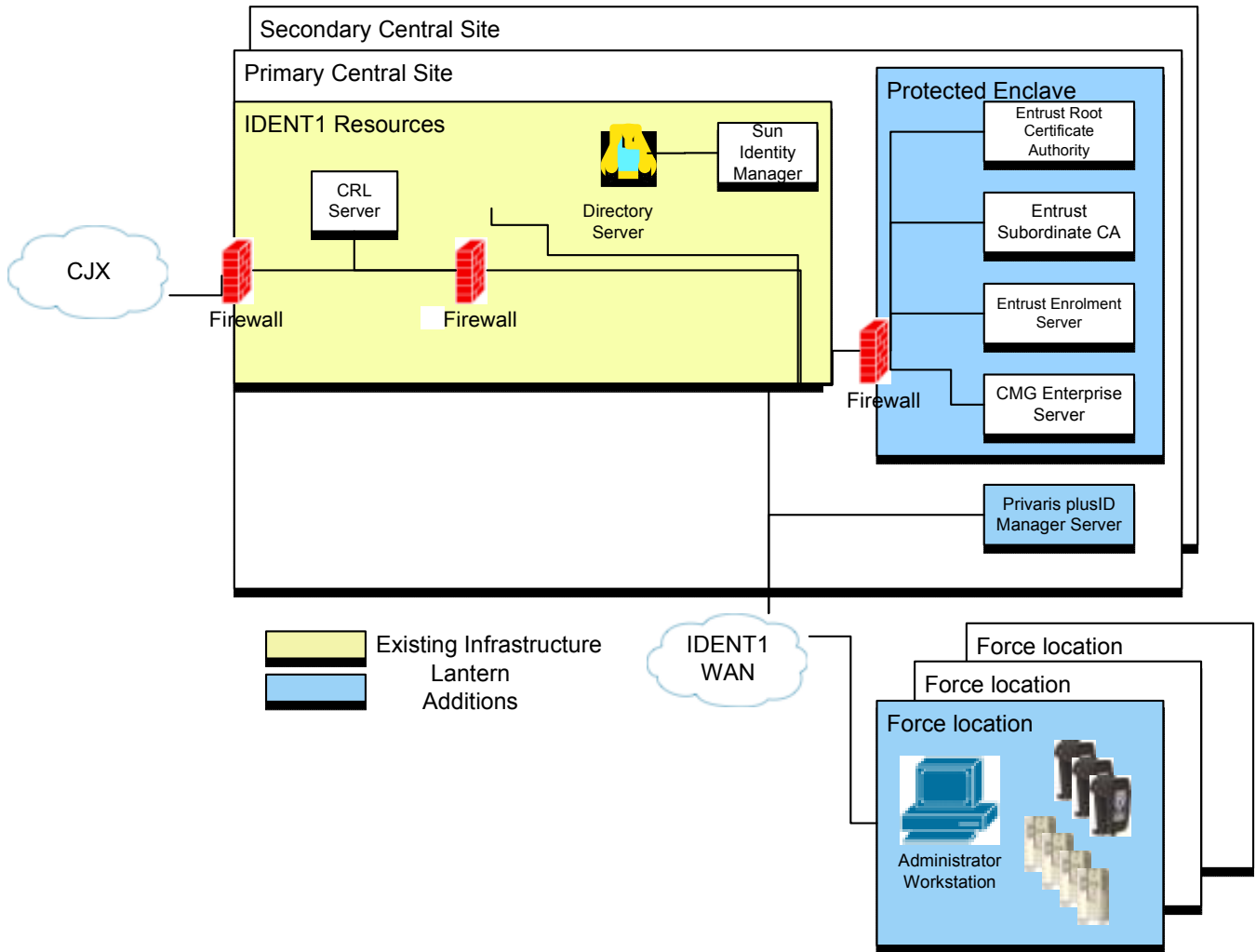


Figure 3-1 Components of the User Authentication Solution

MFRs and Privaris plusID bio-tokens are managed at PC-based Administrator Workstations located at Force locations where Livescan connectivity already exists. Additional equipment is installed at both Central sites to provide resilient central management of both devices as well as for the PKI.

The PKI components, as well as the central CMG policy server are located in a limited access enclave to further protect these security assets. A dedicated Cisco PIX firewall is used for this purpose.

The Entrust PKI is configured with an on-line root Certificate Authority (CA) and a subordinate CA at each central site. Certificate details are replicated between the two sites, ensuring that loss of one CA will not result in loss of certificate information. The Entrust enrolment server provides a web interface for generation of certificates. The CAs use a hardware security module for storage of the root keys.

The Entrust PKI can support many times the number of users required for Lantern. Additional users above that number can be added by acquiring more certificate licenses and Privaris plusIDs or other credentials, such as smart cards. This is an infrastructure component that can be easily extended to other IDENT1 or police uses such as user PC authentication or encryption, and digital signing of documents or e-mail.

The Credant Mobile Guardian (CMG) policy server is also at the Central site, housed within the secure enclave. This is a change from the Pilot, in which it was located outside the Central site across the CJX at a Cable & Wireless facility. Colocating it with other security infrastructure resources tightens control and makes for faster response to problems. The design of the CMG Policy Server is similar to that deployed for the Lantern pilot. However, the latest version of software supporting Windows Mobile 6, and additional Gatekeepers are required to support the number and geographical distribution of MFRs. Updated versions of CMG Shield are also provided for each MFR. This is another change from the Pilot, where these client applications were obtained from C&W by the Authority and CFE to Northrop Grumman.

The Privaris plusID Manager has a similar architecture and has both a Central component and an Administrator Workstation component. The Central PPM server manages and tracks the plusID bio-tokens.

The Administrator Workstation is a PC used for local management. It is an integral part of the solution used to manage both users and devices. The applications loaded on the Administrator Workstation are:

- Credant Mobile Guardian Gatekeeper,
- Privaris plusID Manager client, and
- Entrust Entelligence Security Provider client.

The CMG and Privaris applications have been discussed above. The Entrust ESP is the client application that is used to securely download the user certificates and install them on the Privaris plusID bio-tokens.

3.3 Data Connectivity

The LANTERN Pilot Phase 2 - Implementation Phase utilised General Packet Radio Service (GPRS) connectivity, which was already in use at the selected pilot Forces. The intent was to capitalise on Force investments in mobile data connectivity. Whilst GPRS has performed satisfactorily in the pilot and is the proposed connectivity method for the IDENT1-LANTERN Service Expansion, alternate radio links are under investigation by the Authority and could be adopted in the future for LANTERN. Mobility expansion is proposed to provide the secure communication tunnel needed immediately, use of the best available path, and compatibility with emerging communications methods that may be preferred by the Authority in the future.

3.3.1 Mobility Expansion

An objective of the LANTERN security solution is that it be compatible with a longer term architecture in which the Authority could provide security, mobility and other centralized services in support of mobile data, particularly PDAs. This proposal introduces a mobility client on LANTERN devices which meets current needs and fulfils the objective of long-term compatibility.

The LANTERN devices proposed for the Mobility Expansion also include a new capability for wireless connectivity via an integrated 802.11 (WiFi) modem. Such capability would allow users to take advantage of higher speed connectivity when in the range of WiFi networks (e.g., for future photo transmission). To take advantage of this capability, the devices must have the capability to manage the connectivity among multiple bearers, including the existing GPRS commercial service. The proposed mobility client supports that capability.

A commercial-off-the-shelf (COTS) mobility and security platform will be introduced into the LANTERN network architecture to provide multi-bearer support and compatibility with a more corporate architecture for mobile data. The platform to be introduced is the Apollo Anywhere product from Brand Communications. This is a mature product that is in use by several police forces in the UK and in wide use by mobile workers in the UK utilities industry. The platform consists of a software client that will be loaded on each LANTERN device and a redundant server complex placed behind the IDENT1 firewalls. The platform delivers the following capabilities:

- Seamless operation of LANTERN devices over multiple bearer networks including existing commercial GPRS services, WiFi networks or other networks the NPIA may make available in the future.
- Encryption of data (AES 256-bit code) by establishing a virtual private network between the device and the IDENT1 network.
- End-point security, enabling the device to be remotely disabled if it is determined that the device has been compromised, misplaced or stolen.
- Interoperation with the proposed LANTERN user-level authentication.
- Improved application performance over wireless bearer networks by optimising transmissions and enabling bearer networks to be combined to provide an overall larger bandwidth pipe to applications.

The software client is included in the software image loaded on each LANTERN MFR. The server infrastructure consists of packet access servers for terminating the virtual private network tunnels from each MFR. The packet access servers operate in a dual redundant hot stand-by configuration by virtue of load balancers, with two packet access servers in each data centre. The server complex at each data centre is sized to support the full population of MFRs. The servers run Windows 2003. Management software also resides on the servers for supporting configuration and monitoring of the mobility expansion platform. An additional server is provided at each location to house the SQL database that collects logs and related data from the load balancing/management servers. An assumption is made that the mobility platform interfaces with IDENT1 via a border router. This border router must, in addition to its current configuration, be able to provide a return route for client traffic. The mobility expansion displaces the need for the Aventail VPN client software and service procured from Cable and Wireless by the Authority for LANTERN MFRs in the pilot .

The proposed mobility expansion is architected to initially support exclusively IDENT1, by virtue of the placement of servers inside of the IDENT1 firewall. This architecture enables implementation and deployment before the scheduled deployment of MFRs. However, the solution is scalable in the future should the Authority decide to use the platform to support other mobile device deployments beyond LANTERN and IDENT1.

The Apollo Anywhere client can readily be deployed on other Windows Mobile-based PDAs deployed by other forces and is inherently designed to support a variety of bearer networks. The package access server cluster could be expanded to support additional device quantities, and the clusters relocated outside of the IDENT1 firewall to support broader user access across the CJX. Implementation of the Mobility Expansion to services outside of LANTERN would require additional accreditation work beyond the scope of CCN050.

3.3.2 Subscriber Information Modules (SIM)

A process improvement in the method of implementing subscriber information in the MFR for the specific cellular provider used by the Force receiving the MFR, was adopted in the pilot expansion under CCN040. It centralises the provision of SIMs by the Authority to Northrop Grumman who then manages them centrally and installs them in MFRs prior to shipment. This has proven better than the previous method in which each Force acquired their own SIMs for LANTERN and the installation had to be done at the Force location. Advantages include faster build and setup, lower travel costs, and elimination of the need to open the MFR case repeatedly for each build. The IDENT1-LANTERN Service Expansion will also use this approach.

4. Deliverables

4.1 Non-Document Deliverables

This IDENT1-LANTERN Service Expansion provides the following non-document deliverables:

- LANTERN interface to accept MFR submissions (images or encodings for two to ten fingers) and the central matching facility with updated algorithms within IDENT1 to allow 2 finger print-to-print identification
- Either 1,500 or 2,500 MFRs to access the LANTERN functionality

- Sufficient dedicated search capacity to meet LANTERN search rate of 0.67 per hour per MFR (1000 or 1675 search requests per hour depending on number of deployed MFRs).
- Integration of the MFRs with the Apollo Anywhere client software and Force-supplied GPRS connectivity
- Training of Force IT personnel and trainers of users
- Rollout to a variable number of Forces in accordance with the attached schedule to be confirmed with the Authority consistent with Force availabilities
- Operations and Maintenance (O&M) for all added MFRs deployed to Forces for a period ending 3 years from CCN050 approval.
- 2nd and 3rd line support of the capability for a period ending 3 years from CCN050 approval
- Service management for a period ending 3 years from CCN050 approval
- A secure mobility expansion that supplants the functions of the SRAS consistent with improved communications and security.
- Biometric security for MFRs by requiring a user to authenticate to a bio-token which then enables the device certificate for that user and attaches the identity to all applicable transactions.
- PKI infrastructure that enables the user-level authentication, manages enrolment and other administrative functions, and is integrated with the existing IDENT1 identity management.

4.2 Document Deliverables

This IDENT1-LANTERN Service Expansion provides the following Schedule O (Deliverables) document deliverables:

- Document IDs 1 and 2. Revisions to LANTERN Pilot Phase 2 Test Plan and Procedures
- Document ID 3a. IDENT1-LANTERN Service Expansion Test Readiness Review (TRR) Report
- Document ID 3. IDENT1-LANTERN Service Expansion Test Readiness Review (TRR) Minutes
- Document ID 4. IDENT1-LANTERN Service Expansion Test Summary Report
- Document ID 6. IDENT1-LANTERN Service Expansion Incremental Critical Design Review (CDR)
- Document ID 6. IDENT1-LANTERN Service Expansion Operational Readiness Validation (ORV)
- Document ID 6. IDENT1-LANTERN Service Expansion Operational Readiness Review (ORR)
- Document ID 19. Revisions to LANTERN Pilot Phase 2 Memoranda of Understanding (MOUs)
- Document ID 20. Revisions to LANTERN Pilot Phase 2 Engineering Reports
 - Revisions to Credant Mobile Guardian policy if any
 - Audit and Activity Report (monthly)
- Document ID 26. Revisions to LANTERN Pilot Phase 2 Training Materials for Train the Trainers Day
- Document ID 46. Revisions to LANTERN Pilot Phase 2 Interface Control Document (ICD)
 - Northrop Grumman provided an interface specification for LANTERN pilot searches against the unified fingerprint collection held on IDENT1 in Document CCN009-003-4.0 – LANTERN Interface Control Document (ICD) dated 21 July 2006.
- Document ID 49. LANTERN Service Extension Updates to the Accreditation Documentation Set
- Document ID 60. LANTERN Service Level Requirements (SLR) Report (monthly)

Northrop Grumman and the Authority will determine and agree the content and layout of Document ID's 20 and 26 by the completion of the Incremental CDR.

5. Authority's Responsibilities

Authority's Responsibilities are set out in this clause and it subordinates.

5.1 Customer Furnished Equipment (CFE)/Customer Furnished Information (CFI)

The Authority is responsible for delivery of all CFE/CFI required under this IDENT1-LANTERN Service Expansion:

- Liaison with the Police Forces, and
- All Force GPRS hardware and software for GPRS connectivity.

5.2 Schedule O (Documentation Requirements) Document Review and Approval

It is assumed that Schedule O (Documentation Requirements) document reviews shall be handled on an exception basis where the documents shall be considered "Fit for Purpose" with approval to proceed unless written notice is received by Northrop Grumman not later than ten (10) working days following receipt of the document by the Authority.

6. LANTERN Stakeholders and Responsibilities

Northrop Grumman is the systems integrator and provides the handheld fingerprint capture application, enhanced central search capacity and updated functionality to meet the requirements of this IDENT1-LANTERN Service Expansion

The LANTERN stakeholders and their responsibilities are summarised in Figure 6-1 below.

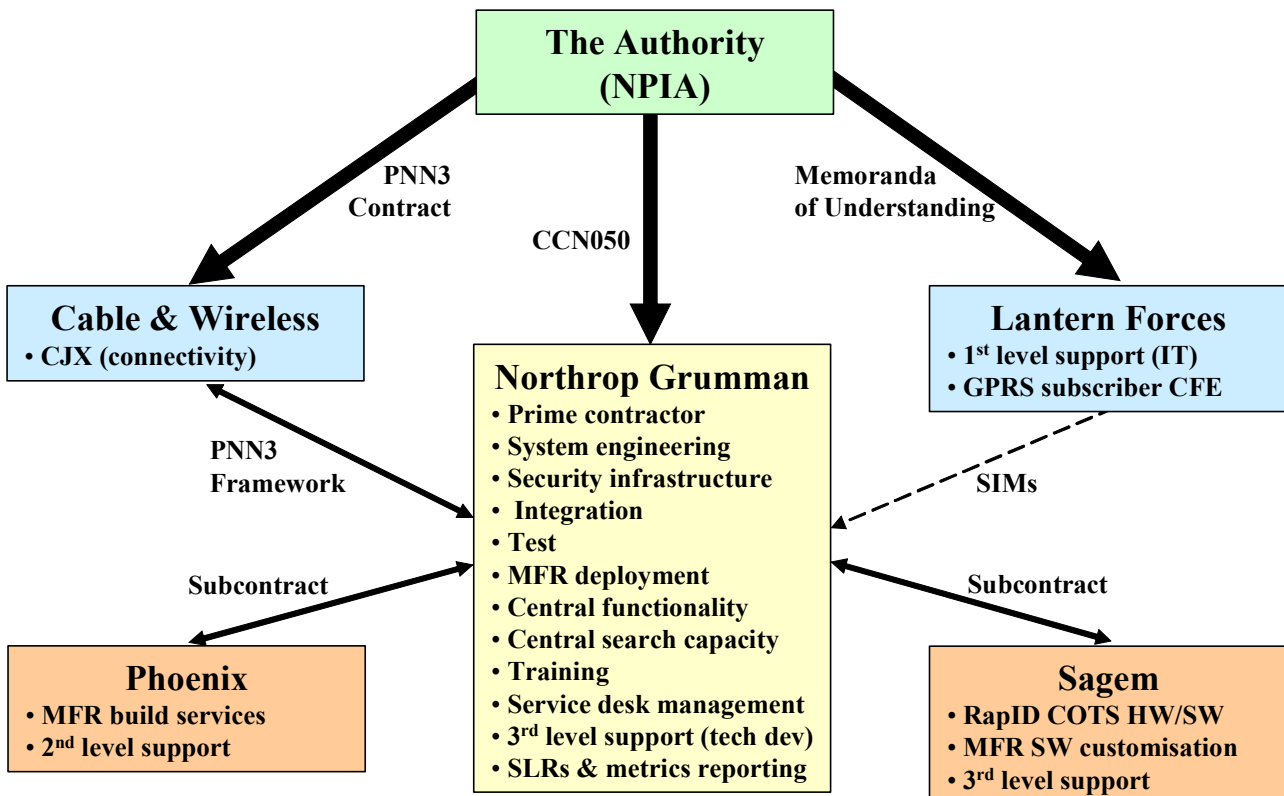


Figure 6-5-1 - LANTERN Stakeholders and Responsibilities

Northrop Grumman is responsible for overall service and service assurance with the exception of the 1st level support to be provided by each Force IT. Force IT shall escalate to the Service Desk only those incidents that

they cannot resolve locally. After that, the Service Desk will manage escalation and tracking of tickets for all incidents. This is illustrated in Figure 6-2.

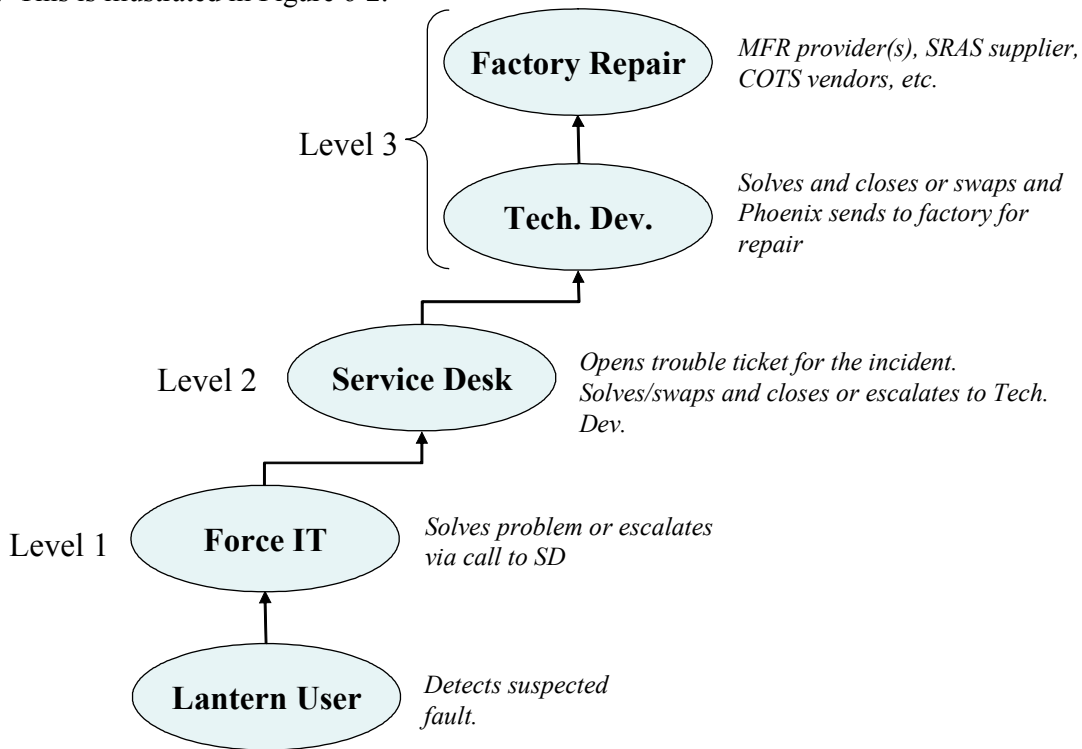


Figure 6-5-2 - LANTERN Service Levels and Responsibilities

7. Schedule

The IDENT1 LANTERN Service Expansion schedule is as set out in Contract Change Note 050R1, Part B-2 “Schedule”. The Schedule is subject to the Clause 9 Assumptions and Conditions.

Milestones to which payments are attached are as shown in the following table.

Milestone	Estimated Month	Acceptance Event	Evidence
Incremental CDR	1	A review of any changes from the design agreed to in the LANTERN Pilot CDR under CCN009.	Completion of the Incremental CDR meeting, acceptance of the presentation materials and minutes
Operational Readiness Validation and Operational Readiness Review	7	Operational Readiness Validation (ORV) and Operational Readiness Review (ORR) held. Review of the status of testing and the results of testing on each requirement, and the status of other pre-requisites for deployment	The ORR and ORV have been held. The delivery of any documents required for the ORV and ORR are not prerequisites for completion of the event.
Start of Deployment	7	MFRs arrive at the first force ready for use in training and operation	MFRs have been shipped to the first Force as identified by the Authority.
50% Completion of Deployment	9 or 10 (depending on quantity)	One-half of the MFRs for which service is contracted under CCN050 have arrived at their respective forces ready	One half of the total quantity of MFRs to be deployed have been shipped to their respective Forces

Milestone	Estimated Month	Acceptance Event	Evidence
	of MFRs)	for use in training and operation	as identified by the Authority.
Completion of Deployment	11 or 13 (depending on quantity of MFRs)	All MFRs for which service is contracted under CCN050 have arrived at their respective forces ready for use in training and operation	All MFRs to be deployed (not including spares) have been shipped to the Forces as identified by the Authority.
Monthly Maintenance	23 months total	Service provided each month starting at completion of deployment + 30 days through end of period of performance	

8. Options

The PNC Warning Flags implementation is priced as an option. Indicative pricing is also provided for one-year extensions of service to follow the 36 month period of performance. Options for extra batteries and chargers for the MFR will be priced when they become available for the third generation device.

9. Assumptions and Conditions

For the purposes of pricing this IDENT1-LANTERN Service Expansion, the following assumptions and conditions apply. Any changes to these assumptions and conditions will be subject to a modification by CCN incorporated through Schedule L (Change Control Procedure).

PNC Warning Flags

- The PNC Warning Flags implementation is dependent upon Back Record Conversion (BRC) being complete. It is assumed that the PNC side of the interface has been developed and commissioned, and that BRC of the PNC WN data has been completed before this capability is deployed.

User Authentication

- 100 Administrator Workstations are deployed to approximately 50 forces at locations with existing IDENT1 WAN connections.
- A maximum of 12,000 users may be enrolled at any one time, with a cumulative maximum of 15,000 unique users during the period of performance as prior users are revoked and new ones are added. Excess beyond this will be handled under change control.
- Accreditation of the User Authentication solution is the responsibility of the Authority.
- The start of deployment of MFRs to forces is contingent on accreditation of the User Authentication solution.

Service Level Requirements

- SLRs are instantiated starting 30 days after completion of MFR deployment under the IDENT1-LANTERN Service Expansion.
- Time to authenticate per search is a negligible added portion of the DMZ in/out response time (estimated to be about one second). This does not include the initial user-level authentication at login.
- The SLR Framework defines two targets for response time distribution: 95% and 90% of responses within 3 minutes. Only 90% is proposed.
- The definition of "DMZ in/out" is given in the SLR Framework (Response time item 2) as, "*Timescale between search entering DMZ/exiting DMZ (NG's area of responsibility).*" The term "exiting" is interpreted to mean "ready to exit upon polling from the MFR." The Central has no control over how long a ready search result waits before it is retrieved by the MFR. The target response time interval must end when the result is ready to be transmitted to the MFR and not include delays in exiting due to GPRS link interruptions, MFR polling cycles, or MFR operation that delays retrieval such as disabling the modem.

- The use of "average" is inconsistent with a % probability of response time meeting the target. An average response time target is a separate and different SLR from the probability distribution metric SLR. Response Time 4 on page 2 of the SLR Framework contains both "average" and a percentage for searches within the response time target. It is interpreted to mean average for the month without the percent.
- Response Time 4 on page 2 of the SLR Framework reduces the target from 3 minutes to 2 minutes. The latter has not been demonstrated. The former (3 minutes) is proposed.
- The added definitions of Service Requests in the SLR Framework, do not have the effect of excluding any service request just because it is an unlisted type, thus escalating it into another category with potentially more stringent targets. Other types of service requests can be raised and will be reported in the overall volume of service requests but the 3.5% SLR only applies to new equipment and training requests.
- Options 2 & 3 of "Other-Service Desk" in the SLR Framework is not proposed. Only Option 1 is proposed, with Force IT continuing to be responsible for Level 1 service.
- The SLR Framework references the "approach for stuck and terminal searches agreed for IDENT1 (CCN016B)?" This had not been agreed as of this writing. Whatever is agreed on this topic for CCN016B will flow down to the SLRs on this CCN.
- The newly added "chase" calls category has a target that we should not receive more than 5% chase-ups (of our total calls to the service desk). Since the nature of incoming calls is not under our control, we agree to report this category but not link it to a financial penalty.
- The calculations for Incident and Problem closure scores now include a "carried forward from previous months" element of the equation. This aspect of the calculation is not included in our proposal. Incidents and problems scoring will be calculated on items raised during the reporting period only.

Programme Related

- The schedule is dependent on the CCN050 approval date being not later than 1 May 2008. Delays risk losing the Sagem factory production slot that has been reserved for Lantern MFRs and could jeopardize the deployment schedule.
- A basis of sizing is an assumed 0.67 searches/hour/MFR. This is consistent with the findings of the Performance and Scalability Report.
- A basis of sizing is an assumed search file sized at 9,975,500. This is the "expected value" from Table 2.7 of the DOR for 2010.
- The baseline design for this CCN has been developed as agreed in accordance with the LANTERN Pilot Phase 2 (CCN009) Critical Design Review. Any changes to that design will be presented at the Incremental CDR. This review focuses on changes due to new requirements such as PNC Warning Flags, SLRs and User Authentication. It does not repeat the presentation of design features from the Pilot, which have been previously accepted.
- There is no formal PDR due to schedule constraints.
- In the absence of a pre-defined deployment model with schedule details, it will be developed by NPIA and is subject to agreement by Northrop Grumman.
- Deployment start is contingent on all previous LANTERN milestones being accepted as fit for purpose and the corresponding invoices paid.
- The Authority will provide subscriber information modules (SIM) needed for installation in the MFRs corresponding to each force.
- The Authority shall provide the liaison with the Forces.

- The Authority shall provide the necessary subscriber information modules (SIM) corresponding to the GPRS carrier of each force where MFRs are deployed for installation in the MFRs. Northrop Grumman's ability to meet the Schedule is dependent on the receipt of CFE/CFI. Accordingly, Northrop Grumman will not be held responsible for any delays to the Schedule due to any delays in receiving CFE/CFI from the Authority beyond the critical dates set forth in the schedule
- Schedule O (Documentation Requirements) document reviews shall be handled on an exception basis where the documents shall be considered "Fit for Purpose" with approval to proceed unless written notice is received by Northrop Grumman not later than ten (10) working days following receipt of the document by the Authority.
- The MFR will only accept index fingers for searching. Alternate fingers will not be tested.
- LANTERN will search the Unified National Collection.
- LANTERN searches will be based on non-verified search architecture.
- LANTERN will use dedicated KBMs separate from other IDENT1 services.
- Extensions beyond the period of performance and technical refresh of MFRs will be provided through the change control process upon the Authority's request.

Annex 1
Annotated Service Level Requirements Framework



NPIA Information and Communications Technology and Science Directorate

Lantern Service Level Reporting / Agreement Requirements Framework

RESTRICTED- COMMERCIAL

Attachment to 08.IDENT1.LGG-097

26th March 2008 (- V1.2)

Author: Brett Boule
NPIA IDENT1 Service Level Manager

Att. B-1, Annex 1
CCN050R1 IDENT1 LANTERN Service Expansion
Page 25 of 50

These commodities, technology or software were exported from the United States in accordance with the Export Administration Regulations. Diversion contrary to U.S. law is prohibited.

RESTRICTED – COMMERCIAL

Purpose

This document aims to identify a framework of NPIA Service Level Requirements for the Lantern service. It has been acknowledged by the authority / supplier that certain requirements may change as a result of ongoing discussions.

The IDENT1 Schedule F part 2 structure will form the basis for the creation of the Lantern Service Level Agreement (SLA). This should incorporate a sliding 10% incentive / credit mechanism.

Service Level Requirements

Category	Requirement	Further Detail / Considerations	Overall SLA Weighting	NG Proposal
Search Volumes	1) To be reported on per Force. Assume used by NPIA to assess utilisation of devices / service Not analysed by NG?	- No SLA financial implication, only reporting requirement by Force	0%	Accepted
Response Times	1) End to End response time reporting required	- No SLA financial implication, only reporting requirement by Force. - End to End refers to time of search launch from MPR / response back to MPR	0%	Accepted
	2) DMZ in / out response time SLA measure required	- SLA financial implication, supporting reporting required. - Measure refers to timescale between search entering DMZ / exiting DMZ (NG's area of responsibility) - User Authentication timescale is presumed part of the DMZ in / out response time. - Clarification required on existing DMZ in / out target response time. - Approach for stuck & terminal searches agreed for	15%	Clarifying assumption provided on definition of DMZ in/out times. 95% response time not

Category	Requirement	Further Detail / Considerations	Overall SLA Weighting	NG Proposal
		<p>IDENT1 (CCN016b) to be carried to Lantern.</p> <p>Revised requirement (both options to be costed)</p> <p>1) 95% within 3 minutes (DMZ in / out which includes authentication)</p> <p>2) 90% within 3 minutes (DMZ in / out which includes authentication)</p>		proposed
	4) DMZ in / out average response time SLA measure required	<p>- SLA financial implication, supporting reporting required.</p> <p>- Measure refers to timescale between search entering DMZ / exiting DMZ (NG's area of responsibility)</p> <p>- Clarification required on existing DMZ in / out average response time.</p> <p>- Approach for stuck & terminal searches agreed for IDENT1 (CCN016b) to be carried to Lantern.</p> <p>Revised requirement (both options to be costed)</p> <p>1) 95% average response time within 2 minutes (DMZ in / out which includes authentication)</p> <p>2) 90% average response time within 2 minutes (DMZ in / out which includes authentication)</p>	15%	NG proposes an average response time target of 3 minutes rather than 2 minutes (DMZ in / out)

Category	Requirement	Further Detail / Considerations	Overall SLA Weighting	NG Proposal
Operational Availability	1) MPR Availability SLA / Reporting requirements.	- No SLA requirement. - Sev 3 (Lantern Device) Incident outage reporting required per force.	0%	Accepted
	2) Central Availability measure is required.	- SLA financial implication, supporting reporting required. - Based on key Hardware & Software / Process Critical Components, (TBA) - Target 99.6% = 100 score SLA target required - Planned / Unplanned downtime. Pre Agreed Maintenance Slots to be used (1 per week, every Wednesday between 2-6am). Any changes to agreed slots / emergency change requirements are to be agreed with Authority / Force. Changes outside maintenance that have not been agreed with the NPIA will be considered unplanned. - 2 weeks notification / approval required on all Planned Downtime, to both Force & Authority. (in writing)	20%	Accepted
Technical Support	1) Receive Call (Calls answered within 60 seconds / ACD measure)	- SLA financial implication, supporting reporting required. - Target 98% = 100 score <u>No of Calls Responded to in 1 min</u> Total ACD calls received for service (to include lost / dropped calls)	7.5%	Accepted
	2) Respond With Status Update	- SLA financial implication, supporting reporting	5%	Accepted

Category	Requirement	Further Detail / Considerations	Overall SLA Weighting	NG Proposal
		<p>required.</p> <ul style="list-style-type: none"> - NPIA requires that this be a “meaningful” update. Definition TBA with NG. The word “meaningful” refers to the supplier providing an update on the progress being made towards resolution of the Incident. This update is to provide additional value & detail than the information provided on first call. - Measurement refers to the time taken for the status update being provided within the required target time. - The content of the status update call will not be formally measured but will be audited by NPIA and any quality issues will be raised through regular service forums. - Changes required as defined in annex 2. - Target 95% = 100 score - Equation proposed = $\frac{\text{No. Incidents resolved within status period (Sev 2 \& 3)} + \text{No. Incidents Status'd (Sev 2 \& 3)}}{\text{Total Incidents (Sev 2 \& 3)}}$		
	<p>3) Service Requests a) Chase Calls</p> <p>Definition - when a User / NPIA contacts the NG service desk to chase-up progress on an existing open Incident, Service Request or Problem.</p> <p>NG need to record the chase-up against the original Service</p>	<p>..... b) - SLA financial implication, supporting reporting required.</p> <ul style="list-style-type: none"> - Target = Chase Calls to be <5% of total volume of open / opened Service request, Incident & Problems for the reporting period - Chase calls to be logged as Severity 0. 	<p>4%</p>	<p>Clarifying assumption provided. Agree to report, but not link to financial accounting.</p>

Category	Requirement	Further Detail / Considerations	Overall SLA Weighting	NG Proposal
	<p>Request, Incident or Problem record within the existing Service Management system (ie. Remedy).</p> <p>.....</p> <p>b)</p> <ul style="list-style-type: none"> - How do I requests - Information Requests (that do not relate to the possible / actual disruption of service) <p>.....</p> <p>c)</p> <ul style="list-style-type: none"> - Training Requests - New equipment requests 	<p>.....</p> <p>b) - No SLA financial implication, only reporting requirement by Force</p> <p>.....</p> <p>- SLA financial implication, supporting reporting required by force. - 95% of requests to receive a estimated lead time / target date to fulfillment and / or quote (as required) within 5 days of the initial request being raised.</p>	<p>0%</p> <p>3.5%</p>	
	<p>3) Incident Resolution) <u>Incidents (definition):</u></p> <ul style="list-style-type: none"> - Any unplanned interruption to an IT service or reduction in the quality of an IT service. - Any failure or unauthorised change to a configuration item that impacts or has the potential of impacting service should be classified as an incident. 	<ul style="list-style-type: none"> - SLA financial implication, supporting reporting required. - Severity definition Changes required as defined in annex 1. - Equation proposed = <p style="text-align: center;">Number of Incidents & Service Requests resolved within Target Time for reporting period</p>	<p>20%</p>	<p>Clarifying assumption provided in relation to incidents carried from previous reporting</p>

Category	Requirement	Further Detail / Considerations	Overall SLA Weighting	NG Proposal
	<ul style="list-style-type: none"> - Any disruption to service that impacts or has the potential of impacting the users ability to use the service. - The proactive identification of errors within the system / internal errors detected by the supplier should be logged as either a Incident or Problem. - There should be no "internal incidents", all internal errors should be logged as Incidents. Any event / alerts that are identified via system management tools that either impacts or has the potential of impacting service should also be recorded and counted as an incident. For clarification an event / alert will become a Incident once the agreed system / infrastructure performance thresholds have been exceeded. Any events / alerts that are identified but do not represent a risk to service are logged and reported separately for each reporting period. SLA measures do not apply to this category of remedy tickets. - The NPIA and Users should be informed of all incidents via agreed channels. - Lost / broken equipment would also be captured and resolved as a Incident. - Lost passwords / password resets are to be captured as Incidents. - Anything else that isn't classified as either an Incident, Service Request or Problem should be captured as a Incident, (excludes operational changes and event / alerts). 	<p>----- Total Incidents & Service Requests raised for reporting period + Open Incidents / SR's carried from previous reporting period</p> <ul style="list-style-type: none"> - Target 95% = 100 score - All categories of Service Request to be defined / agreed up front. Anything not defined as Service Request is to be considered an Incident. - Incident / Service Request SLA failures are to be carried forward / cumulative for reporting periods. Open Incidents that have failed SLA are to be counted against future SLA reporting periods until resolved. 		periods
	4) Problem Management	- SLA financial implication, supporting reporting required.	10%	Clarifying assumption

Category	Requirement	Further Detail / Considerations	Overall SLA Weighting	NG Proposal
		<p>- “Workaround” & “Resolution” requirements apply - Resolution Target 95% = 100 score - Workaround Target 90% = 100 score - Equation proposed =</p> $\frac{\text{Number of Problems Resolved within Target Time for reporting period}}{\text{Total Problems Raised for reporting period + Open Problems carried from previous reporting period}}$ $\frac{\text{Number of Workarounds provided within Target Time for reporting period}}{\text{Total Problems Raised for reporting period + Open Problems carried from previous reporting period}}$ <p>- Problem Severity definition as defined in annex 3. - Problem SLA failures are to be carried forward / cumulative for reporting periods. Open problems that have failed SLA are to be counted against future SLA reporting periods until resolved. - For those problems which have a defined workaround but cannot be applied / fixed due to reliance on a future Release the option of “freezing” the time clock is to be agreed with the NPIA. Problems deemed to be low priority may also be “frozen” under exceptional circumstances. In all cases NG will seek the prior approval of the NPIA before any problems are “frozen”.</p>		<p>provided in relation to problems carried from previous reporting periods</p>

Category	Requirement	Further Detail / Considerations	Overall SLA Weighting	NG Proposal
Matcher Quality / Accuracy	“Seed Data” approach to be adopted as defined with Lantern Shadow Metrics Report.	- No SLA financial implication, only reporting requirement	0%	Accepted
Other				
Service Desk	Service Desk Model (3 Options to be costed against) All 3 options are to be costed.	<p><u>Option 1</u> - Level 1 = Force IT Support - Level 2&3 = NG / Service Desk</p> <p><u>Option 2</u> - Level 1 = NG / Service Desk, 5pm – 9am - Level 2&3 = NG / Service Desk</p> <p><u>Option 3</u> - Level 1, 2 & 3 = NG / Service Desk, 24/7</p>	N/A	Clarifying assumption provided. Only Option 1 is proposed

Annex 1

Incident Severity Level	Title	Description
0	Service Request & Chase Calls	<p>All system or service matters that do not equate to an incident, e.g., advice or guidance. This will include all contacts to the Service Desk that do not fall into one of the other severity levels.</p> <p>Chase Calls relate to when a User / NPIA contacts the NG service desk to chase-up progress on an existing open incident, service request or problem.</p>
1	Non-critical Incident	Incidents affecting non-critical Lantern hardware and software capabilities that do not cause a loss of Lantern Services.
2	Central Segment Incident	Incidents affecting critical Central Lantern hardware and software / processes
3	Lantern Incident	Incidents causing a loss of Lantern device services.

Annex 2

Incident Severity Levels	Response Levels		
	1 (Receive Call)	2 (Respond with Update)	3 (Resolution)
0 – Service Request & Chase Calls	1 Minute	5 Days (Category C Service Requests, requirement defined above)	None
1 – Non-critical Incident	1 Minute	n/a	24 Hours
2 – Central Segment Incident	1 Minute	30 Minutes	3 Hours
3 – Lantern Incident	1 Minute	60 Minutes	24 Hours

Annex 3

Problem Severity Levels	Response Levels		
	1 (Receive Call)	2 (Workaround)	3 (Resolution)
1 – Non-critical Problem	n/a	(Low priority, within 21 days) (Medium priority within 14 days) (High priority within 7 days)	(Low priority, within 45 days) (Medium priority within 28 days) (High priority within 21 days)
2 – Central Segment Problem	n/a	(Low priority, within 7 days) (Medium priority within 5 days) (High priority within 3 days)	(Low priority, within 28 days) (Medium priority within 21 days) (High priority within 14 days)
3 – Lantern Device Problem	n/a	(Low priority, within 21 days) (Medium priority	(Low priority, within 35

		within 10 days) (High priority within 5 days)	days) (Medium priority within 28 days) (High priority within 21 days)
--	--	---	---

Annex 2

IDENT1 LANTERN Service Expansion

Requirements Set

Requirement	Response
1 Capture	
2 Transmission and Storage	
Send and Receive	The three Pilot requirements in this section that were not met were by agreement with the Authority in order to reduce licence costs and keep the MFR as non-proprietary as possible.
<p><i>ID</i> : Req55 <i>Type</i> : Pilot Req The MFR shall be able to send encoded fingerprints to the IDENT1-LANTERN interface. <i>Delivered</i> : Please Confirm <i>Delivery Planned for</i> : PILOT</p>	Not proposed. It is in the generic Sagem RapID, but the LANTERN customisation does not support. The fingerprint encoder used must be the Sagem encoder to keep it in sync with the matcher software.
<p><i>ID</i> : Req3 <i>Type</i> : Pilot Req The IDENT1-LANTERN interface shall receive encoded fingerprints. <i>Delivered</i> : Please Confirm <i>Delivery Planned for</i> : PILOT</p>	Accepted. Test passed in Pilot
<p><i>ID</i> : Req21 <i>Type</i> : Pilot Req It shall be possible to configure the MFR to send either encodings of fingerprint images or compressed fingerprint images to the IDENT1-LANTERN interface. <i>Delivered</i> : Please Confirm <i>Delivery Planned for</i> : PILOT</p>	Not proposed. It is in the generic Sagem RapID, but the LANTERN customisation does not support. The use of images rather than encoded minutiae was done to keep licensing costs down and to make sure the interface was compatible with any MFR.
<p><i>ID</i> : Req46 <i>Type</i> : Pilot Req The MFR shall send to IDENT1, and IDENT1 shall receive from the MFR, fingerprint encodings to the ANSI/NIST- ITL-2000 Data Format for the Interchange of Fingerprint, Facial and SMT Information Standard, Version 4, using a Type 9 logical record. <i>Delivered</i> : Please Confirm <i>Delivery Planned for</i> : PILOT</p>	Not proposed. It is supported in the ICD & LANTERN Central, but not the MFR. The use of images rather than encoded minutiae was done to keep licensing costs down and to make sure the interface was compatible with any MFR.
Communications	
<i>ID</i> : Req36	Accepted. Passed in current pilot.

Requirement	Response
<p><i>Type</i> : Pilot Req The MFR shall encode or compress, process and initiate the transmission of the fingerprint image(s) in less than one second. <i>Delivered</i> : Please Confirm <i>Delivery Planned for</i> : PILOT</p>	
<p><i>ID</i> : Req71 <i>Type</i> : Pilot Req The IDENT1-LANTERN interface shall retain GPS co-ordinates to provide an accurate record of where prints were taken. <i>Delivered</i> : No <i>Delivery Planned for</i> : CCN050</p>	Accepted. This is in the ICD. It will have to be parsed and tracked in the Data Warehouse. Audit additions and updates are also proposed.
<p><i>ID</i> : Req270 <i>Type</i> : New Req The MFR shall support the sending of GPS co-ordinates to the IDENT1-LANTERN interface to record an accurate location for every search. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	Accepted. The PDA/Smartphone used in the 3 rd generation RapID has a GPS receiver. Sagem needs to modify the MFR software application to send the geo-location of the device with the search request.
3 Search	
4 Response	
Respondent Information	
<p><i>ID</i> : Req8 <i>Type</i> : Pilot Req The IDENT1-LANTERN interface shall return relevant PNC information. including PNC Warning Flags, Name, DOB, Sex and unique identifier (e.g. CRO, URN). <i>Delivered</i> : Partly <i>Delivery Planned for</i> : PILOT</p>	<p>Accepted. All but PNC Warning Flags were tested and passed in the pilot. PNC Warning Flags included in proposed option.</p> <p>Dependant on PNC completing their interface in accordance with the ICD delivered previously by Northrop Grumman.</p>
<p><i>ID</i> : Req105 <i>Type</i> : Pilot Req The value of the Warning flags shall be displayed using the PNC Codes rather than any long description. <i>Delivered</i> : No <i>Delivery Planned for</i> : CCN050</p>	Accepted. PNC Warning Flags included in proposed option
<i>ID</i> : Req294	Accepted. PNC Warning Flags

Requirement	Response
<p><i>Type</i> : New Req The MFR shall display a 'WM' (Wanted Missing) to indicate any return of any type of Report Class in the PNC Warning Message. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	<p>included in proposed option</p>
<p><i>ID</i> : Req295 <i>Type</i> : New Req The MFR shall display the first two letters of agreed Warning Signals, as part of the PNC Warning Message, that are associated to each result, such as: 'FI' - Firearms 'WE' - Weapons 'VI' - Violent 'ES' - Escaper 'SU' - Suicidal 'SH' - Self-Harm 'DR' - Drugs <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	<p>Accepted. PNC Warning Flags included in proposed option</p>
<p><i>ID</i> : Req296 <i>Type</i> : New Req The MFR shall display the Warning Marker Message for the Report Class and Warning Signals above the CRO number on the HCI in the following format: WM-<WS>-<WS>-<WS>-<WS>-<WS>-<WS>-<WS> e.g 1. WM-FI-WE-VI-ES-SU-SH-DR CRO 1234567 e.g. 2 WM-WE-VI-DR CRO 1234568 <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	<p>Accepted. PNC Warning Flags included in proposed option</p>
<p><i>ID</i> : Req297 <i>Type</i> : New Req The MFR shall display the agreed Information Markers from the PNC Warning Message that</p>	<p>Accepted. PNC Warning Flags use of two-character codes as defined in the Phoenix System Data Definitions is included in the</p>

Requirement	Response
<p>are associated to each result, in a format to be determined. <i>Delivered :</i> <i>Delivery Planned for :</i> CCN050</p>	<p>proposed option.</p>
<p><i>ID :</i> Req288 <i>Type :</i> New Req The MFR shall be able to receive responses to searches from the LANTERN interface when the device is locked and not turned off. This applies to MFRs that have a User Authenticated to the MFR and LANTERN interface who have not completely logged off the MFR. <i>Delivered :</i> <i>Delivery Planned for :</i> CCN050</p>	<p>Accepted. The approach depends on how the new version of CMG works and that the data can be encrypted at rest for a single user, with no other users having access. “Locked” with respect to CMG means just protected by the authentication (PIN) screen. All programs continue to run, data is not encrypted on lock. It is just an inactivity timer. We will resolve any Sagem application issues with the encryption of data.</p>
<p><i>ID :</i> Req289 <i>Type :</i> New Req The MFR shall display all results received on the MFR that have not been deleted, to the User when the same User unlocks the MFR. <i>Delivered :</i> <i>Delivery Planned for :</i> CCN050</p>	<p>Accepted. The approach depends on how the new version of CMG works and that the data can be encrypted at rest for a single user, with no other users having access. We will resolve any Sagem application issues with user access to data.</p>
<p><i>ID :</i> Req290 <i>Type :</i> New Req The MFR shall display all results received on the MFR that have not been deleted, to any User who is authorised to see the data once they have been through the user authentication process on the specific MFR. <i>Delivered :</i> <i>Delivery Planned for :</i> CCN050</p>	<p>Accepted. The approach depends on how the new version of CMG works and that the data can be encrypted at rest for a single user, with no other users having access. We will resolve any Sagem application issues with user access to data.</p>
<p><i>ID :</i> Req291 <i>Type :</i> New Req The MFR shall deny access to results that the User does not have authority to view. <i>Delivered :</i> <i>Delivery Planned for :</i> CCN050</p>	<p>Accepted. The approach depends on how the new version of CMG works and that the data can be encrypted at rest for a single user, with no other users having access. We will resolve any Sagem application issues with user access to data.</p>
<p><i>ID :</i> Req292 <i>Type :</i> New Req</p>	<p>Accepted. The approach depends on how the new version of CMG</p>

Requirement	Response
<p>An Authenticated User shall be able to delete any results stored on the MFR. <i>Delivered :</i> <i>Delivery Planned for :</i> CCN050</p>	<p>works and that the data can be encrypted at rest for a single user, with no other users having access. We will resolve any Sagem application issues with the encryption of data. Best practice would be for a user to delete all results before logging off and disallow two users from being logged on or using the same MFR concurrently.</p>
5 Watch Lists	
6 Battery Requirements	
7 Security	
Access Control	
<p><i>ID :</i> Req228 <i>Type :</i> New Req Access to the MFR and the IDENT1-LANTERN interface shall be protected by a secure authentication service. The authentication service shall maintain identification and authentication data in a protected form. <i>Delivered :</i> <i>Delivery Planned for :</i> CCN050</p>	<p>Accepted. Proposed as User Authentication.</p>
<p><i>ID :</i> Req12 <i>Type :</i> Pilot Req The Supplier shall ensure that a user based authentication service is provided for the MFR and the IDENT1-LANTERN interface. <i>Delivered :</i> No <i>Delivery Planned for :</i> CCN050</p>	<p>Accepted</p>
<p><i>ID :</i> Req237 <i>Type :</i> New Req Access to the IDENT1-LANTERN interface shall be role based . <i>Delivered :</i> <i>Delivery Planned for :</i> CCN050</p>	<p>Accepted. Users are IDENT1 users with LANTERN role.</p>

Requirement	Response
<p><i>ID</i> : Req260 <i>Type</i> : New Req It shall be possible for LANTERN users to belong to more than one IDENT1 role group. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	Accepted
<p><i>ID</i> : Req238 <i>Type</i> : New Req Access to functions and associated data provided by the LANTERN-IDENT1 interface shall be based on user permissions. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	Accepted
<p><i>ID</i> : Req251 <i>Type</i> : New Req Functions provided by the LANTERN-IDENT1 interface which users do not have permission to access shall not be displayed to them. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	Accepted
<p><i>ID</i> : Req277 <i>Type</i> : New Req The Supplier shall provide the Police Forces the capability to directly enroll Users to the Lantern System. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050 OK - planned with IdM and the administrator workstation</p>	Accepted. Approach uses IDENT1 Identity Management and Administrator Workstations.
<p><i>ID</i> : Req280 <i>Type</i> : New Req The Supplier shall provide the Police Forces the capability to directly maintain the Roles and Users of the Lantern System. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	Accepted. Approach uses IDENT1 Identity Management and Administrator Workstations.
<p><i>ID</i> : Req276 <i>Type</i> : New Req The Supplier shall develop a user authentication solution that is device agnostic. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	Accepted. Certificates are standards-based and can be used on any device supporting the standards.

Requirement	Response
<p><i>ID</i> : Req236 <i>Type</i> : Inf User authentication may be possible by the following methods or a combination of:</p> <ul style="list-style-type: none"> • ID and Password •User's Fingerprint •Smartcard •Token <p><i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	<p>Accepted with the proviso that “or” is interpreted to mean the requirement is met if authentication is by one or more of the bulleted items, but not necessarily all of them individually or in combination. The proposed user authentication approach provides authentication by means of token and user’s fingerprint, but not ID and password or smartcard.</p>
<p><i>ID</i> : Req278 <i>Type</i> : New Req The Supplier shall develop a user authentication process where the initial authentication will take no more than one minute. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	<p>Accepted. This covers authentication only, not the decrypting of data or other subsequent steps. We estimate it will take less than 10 seconds for authentication to the MFR.</p>
<p><i>ID</i> : Req279 <i>Type</i> : New Req The Supplier shall develop a user authentication process where subsequent log-ons to a specific MFR are instant for a user that has been initially authenticated and not logged off completely for that MFR. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	<p>Accepted with the understanding that “not completely logged off” means the device is locked due to inactivity but the user has not ended the session and no other user has tried to log on.</p>
<p><i>ID</i> : Req285 <i>Type</i> : New Req Any Authorised Lantern User of an MFR shall be able to authenticate themselves to any one MFR at a given moment in time. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	<p>Accepted with the understanding that this means at “least one MFR” at a given moment in time, not “only one” at a time. The proposed approach provides the capability to pair the token with up to four different MFRs. This gives a user the ability to authenticate to up to four MFRs, although this could be prohibited procedurally through training.</p>
<p>Security Management</p>	
<p><i>ID</i> : Req271 <i>Type</i> : New Req Stored data and configuration data held on the MFR shall be protected from unauthorised use and meet HMG standards.</p>	<p>Cannot categorically agree to “meet HMG standards” because no specific standards are identified. The intent is to meet the necessary standards for protecting stored data</p>

Requirement	Response
<p><i>Delivered :</i> <i>Delivery Planned for :</i> CCN050</p>	<p>and configuration data held on the MFR. The proposal includes the use of the CLAS consultant to assist in this area.</p>
<p><i>ID :</i> Req282 <i>Type :</i> New Req The Supplier shall take due consideration of HMG Information Assurance Policy as embodied in the ACPO community security policy for any proposed user authentication solution.</p> <p><i>Delivered :</i> <i>Delivery Planned for :</i> CCN050</p>	<p>Accepted</p>
<p><i>ID :</i> Req283 <i>Type :</i> New Req The Supplier shall ensure that the user authentication solution undergoes Accreditation prior to implementation of the solution.</p> <p><i>Delivered :</i> <i>Delivery Planned for :</i> CCN050</p>	<p>Accepted with the proviso that the Authority is responsible for arranging accreditation.</p>
<p><i>ID :</i> Req284 <i>Type :</i> New Req The Supplier shall ensure that the solution is subject to the 'IT Health Check' as part of the accreditation.</p> <p><i>Delivered :</i> <i>Delivery Planned for :</i> CCN050</p>	<p>Accepted. Three IT Health Checks are proposed for the Privaris device, the MFR and the Lantern interface.</p>
<p><i>ID :</i> Req263 <i>Type :</i> New Req There shall be an enrolment process to allow the MFR to communicate with the IDENT1-LANTERN interface.</p> <p><i>Delivered :</i> <i>Delivery Planned for :</i> CCN050</p>	<p>Accepted. This is part of the CMG setup. Device management at the interface is provided by CMG inside IDENT1.</p>
<p><i>ID :</i> Req264 <i>Type :</i> New Req Every MFR shall be registered through an enrolment process prior to use.</p> <p><i>Delivered :</i> <i>Delivery Planned for :</i> CCN050</p>	<p>Accepted. This is provided through CMG.</p>
<p><i>ID :</i> Req266</p>	<p>Accepted.</p>

Requirement	Response
<p><i>Type</i> : New Req In the event of decommissioning, the MFR shall be deregistered and returned to a factory fresh state. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	
Audit	
<p><i>ID</i> : Req231 <i>Type</i> : New Req All users of the service shall have a unique identifier against which auditable events shall be recorded in a security event audit log. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	Accepted.
<p><i>ID</i> : Req232 <i>Type</i> : New Req The following <i>basic</i> IDENT1-LANTERN interface security related events shall be recorded in the audit log:</p> <ul style="list-style-type: none"> • log-in attempts; • log-out (both manual and automatic); • creation, deletion or alteration of user accounts/user groups; • creation, deletion or alteration of passwords; • creation, deletion or alteration of access rights/roles; • creation, deletion or alteration of accounting logs. <p><i>Delivered</i> : <i>Delivery Planned for</i> : CCN050</p>	Accepted
<p><i>ID</i> : Req252 <i>Type</i> : New Req For all security related events recorded in the audit log, associated recorded information shall include:</p> <ul style="list-style-type: none"> • date and time of event; • user; • event; • success or failure plus supporting information where appropriate e.g. “failed log-in due to 3 failed previous attempts”; • device on which event occurred; • associated data. <p><i>Delivered</i> :</p>	Accepted

Requirement	Response
<i>Delivery Planned for</i> : CCN050	
<i>ID</i> : Req233 <i>Type</i> : New Req Each search request, including those spawned within IDENT1, shall be logged with a unique transaction identifier. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050	Accepted. Required by LANTERN Pilot ICD.
<i>ID</i> : Req274 <i>Type</i> : New Req Each search request, including those spawned within IDENT1, shall be logged with the User Identification ID and the unique Device ID. <i>Delivered</i> : <i>Delivery Planned for</i> : CCN050	Accepted. Part of User Authentication.
8 Usability	
<i>ID</i> : Req24 <i>Type</i> : Pilot Req MFRs that are capable of capturing images, shall be able to take a photo of an individual so the user can associate a LANTERN identification request on the device to the individual concerned and to link it to the response. <i>Delivered</i> : No <i>Delivery Planned for</i> : CCN050	This requirement came in too late to be included in the CCN050R1 proposal. The proposed MFR does have a camera, but the LANTERN application does not provide for capture and display with it. Therefore, it requires changes to our subcontract with Sagem. We are happy to discuss this with the Authority and add the small expected cost under change control.
9 Service Delivery and Support	
<i>ID</i> : Req243 <i>Type</i> : Inf Service provision will be primarily managed according to an Operational Service Level Agreement (Operational SLA). This SLA will be agreed between the Supplier and NPIA at the start of CCN050 and will cover the services and service levels to be delivered. <i>Delivered</i> : <i>Delivery Planned for</i> :	Accepted
Service Performance and Accuracy	
<i>ID</i> : Req206 <i>Type</i> : Pilot Req The end to end Response Time shall be no	Accepted

Requirement	Response
greater than five minutes. <i>Delivered</i> : Continuing Requirement <i>Delivery Planned for</i> : PILOT	
Service Level Management	
<i>ID</i> : Req215 <i>Type</i> : Pilot Req MIS reports shall be produced at agreed intervals. The MIS reporting shall include both SLA measurements and data provided to assist in the monitoring of the operational use of the device(s), and effectiveness of different devices. <i>Delivered</i> : Continuing Requirement <i>Delivery Planned for</i> : PILOT	Accepted. The proposal includes building on the Pilot capabilities by consolidating data from multiple sites, servers and tables, adding data to the Data Warehouse, and developing the capability to generate reports either from Discoverer or as Oracle Reports.
Service Support	
<i>ID</i> : Req209 <i>Type</i> : Pilot Req The Supplier shall provide a Help Desk facility to immediately de-register devices, available 24/7, in the event of loss/theft. <i>Delivered</i> : Continuing Requirement <i>Delivery Planned for</i> : PILOT	Accepted
<i>ID</i> : Req211 <i>Type</i> : Pilot Req The Supplier shall provide Help Desk support to the Force IT department available 24/7 for the central matching system and IDENT1/CJX gateway. <i>Delivered</i> : Continuing Requirement <i>Delivery Planned for</i> : PILOT	Accepted
<i>ID</i> : Req212 <i>Type</i> : Pilot Req The Supplier shall manage and own all support calls from the Force IT Help Desk, including the liaison with C&W where applicable to resolve issues that relate, or potentially relate, to the VPN SRAS solution and its use in the MFR facility. <i>Delivered</i> : Continuing Requirement <i>Delivery Planned for</i> : PILOT	Accepted. VPN SRAS solution has been supplanted by Mobility Expansion, and any calls from Force IT relating to it will be owned by the Northrop Grumman Service Desk.
10 Training	
<i>ID</i> : Req275 <i>Type</i> : New Req The Supplier shall maintain and update the training materials provided for end users.	Accepted. Additional training has been proposed. It will use existing published training materials and computer-based training (CBT).

Requirement	Response
<i>Delivered :</i> <i>Delivery Planned for :</i> CCN050	