Document Name	**Lantern Project – The Way Forward**
File Name	IDT004-0101-project way forward- project board recommendations 080403 v1.0
Author	[redacted] Biometric Operations and Implementation Manager

Authorisation	
Signed version held by	

Table of Contents

1. Controlling documents 3

2. Background 4

3. Changes in Sensor Technology 5

4. User Authentication 6

5. Re-Examination of Options 1-3 8

6. Issues to be considered if Option 2 is taken forward. 10

7. The constants regardless of option chosen 11

8. Critical Success Factors 12

9. Additional considerations and opportunities 12

10. Control page 14

11. Annex A 15

12. Appendix B 16

1. Controlling documents

This section will contain reference to any source material used in the preparation of the document. This should include reference to relevant standards or guides.

Description	Document number	Revision
Northrop Grumman CCN 050R1 proposal	08.IDENT1.LGG-097 31st March 08	1
Project Board paper July 2007	IDT004-118-0302-Project Options National Rollout 070622v0.3	

2. Background

On 28th June 2007 the project board were asked to consider 3 national procurement options to decide the way forward for the Lantern project.

The options considered at that time can be summarised thus:-

NATIONAL PROCUREMENT OPTION 1
Keep same device and provider and expand to all forces

NATIONAL PROCUREMENT OPTION 2
Keep the Fingerprint Database with IDENT1, and use devices provided by other multiple suppliers

NATIONAL PROCUREMENT OPTION 3
Fingerprint Matching service and devices provided by independent companies. IDENT1 provides database with 'raw' fingerprint data.

The project board agreed that Option 2 was the preferred way forward at that time. [G:\02 - Registered Files\118 - Project Management\101 - Projects\LANT - LANTERN Project\104 - Project Board\IDT004-0101-PB6 Minutes 070724 V1 0-118-101-LANT-104.doc]

In November 2007, CC Peter Neyroud, the NPIA CEO, requested the project team to look at the feasibility of deploying up to [redacted] devices of the type currently used in the Lantern pilot, out to all forces, as an 'interim' solution whist continuing to develop the 'final' solution.

This interim approach was effectively Option 1 above, but limited the numbers of devices deployed.

This request was examined by the project team, and a costed proposal received from Northrop Grumman (CCN050). The proposal was considered to be uneconomic for an interim solution. This position is discussed in greater detail in the NPIA report "CCN050 Evaluation and Project Board Recommendations" dated 3 April 2008

In light of the above and rapid advances in technology that could not have been considered as part of the original options paper, it is now prudent to consider the options once again, to ensure that the correct strategy is chosen to deliver the right solution, in the right time, in the right manner.

3. Changes in Sensor Technology

The size of a mobile fingerprinting device is governed by the type of fingerprint censor utilised in its construction.

The types of sensors that can be used in mobile devices essentially fall into three categories. Prismatic Optical, Thin film Optical and Capacitive.

(Please see Annex A for descriptions of these types of sensor.)

At the time of writing the previous options paper, the industry was advising that the only viable mobile fingerprinting sensor for the type of work it was needed for (1 to many searches) was a prismatic based optical reader. The reasons for this being that the thin film optical and capacitive sensors lacked the necessary accuracy and were only suitable for 1 to 1 verification work.

Although very accurate, prismatic optical sensors are by necessity, very bulky in their construction, and as such their size will ultimately dictate the overall size of the devices they are built into. Such a sensor also has a high power consumption so any portable device has to have sufficient battery power to meet user requirements (e.g. lasting longer than one shift).

Thin film optical, and capacitive sensors are much smaller (much the same area as a large postage stamp), and have a lower power consumption need.

The device used in the pilot uses a prismatic optical reader.

The combination of sensor size and the high power battery produced a bulky, but relatively light device. However it does not lend itself to being carried easily on non-vehicle related duties.

User feedback requires any future fingerprint device to be smaller and lighter, and if possible, be incorporated into existing portable data devices, or made available as a peripheral piece of equipment.

The key to meeting the user need for smaller devices or small peripheral devices such that can connect to, for example, PDA's or police radios, is a suitable capacitive or thin film sensor.

Towards the end of 2007, the project team became aware that a particular capacitive sensor (made by a company called UPEK), had been approved by the FBI for personal identification verification (PIV) operations.

Although this is a 1 to 1 process, the FBI report on the sensor indicated that it could be suitable for a 'lights out'[1] 1 to many process.

In terms of progress for the project, a capacitive sensor that is as good as a prismatic optical sensor, would effectively open a 'Pandora's box' of opportunity for both police forces, and industry, to seek out innovative solutions to their fingerprinting needs.

It is therefore important to examine the viability of the capacitive sensor for the project needs, and work is proposed to ascertain that. (see Annex B – executive summary of document by Ambika Suman ***"Lantern Technical Options Paper – evaluation of fingerprint sensor technologies".***)

It is anticipated that the work proposed within that document could be completed by the end of July 2008 and some preliminary work has already been undertaken to take this proposal forward.

If the capacitive sensor fails to meet accuracy requirements, the only devices that could be utilised in a national solution would be prismatic optical senor based devices or peripherals.

RECOMMENDATION 1

The project board approve the work to be undertaken by the proposal in the Lantern Technical Options Paper – evaluation of fingerprint sensor technologies. That work to be completed by the end of July 2008.

4. User Authentication

The principal key to delivering mobile fingerprinting on a national scale is the need to meet the security requirements of IDENT1.

IDENT1 has a requirement to be able to identify every individual user accessing the system, and to determine not only if the user is allowed to use the system, but to establish if the user is authorised to receive the information being returned to them.

The Lantern pilot received a dispensation from the National Security Accreditor to use device level authentication, with the rider that this solution could not be used in any national solution.

It needs to be clearly understood that, for ANY national solution to provide a mobile fingerprint identification capability, user level authentication HAS to be in place, unless the need for that level of authentication is removed

[1] This is the term used to signify a machine to machine based check, without human intervention

as a mandatory requirement of accessing IDENT1 (which is not a realistic option) or user authentication is addressed elsewhere in the process.

UPSA (Unified Police Security Architecture)[2] (now IAM – Identity and Access Management) could possibly provide the level of authentication needed but may not do so in the time frame needed for this project

User level authentication does not necessarily have to be performed within IDENT1. For instance, if fingerprint checks were carried out via a "gateway" and that gateway also carried out the authentication, and was trusted by IDENT1, then the transaction could proceed.

Research indicates that the Mobile Identification project had in their initial vision a single, national, gateway designed to handle all transactions from mobile devices and the various databases they need to connect with as part of the police officers day to day duties.

Mainly due to the urgency of the Government's demand to get 10,000 mobile data devices out to forces by September 08, the Mobile Information project have now abandoned this approach in favour of a policy of assisting forces, or groups of forces, to produce their own gateways.

The agreed architecture for these gateways require them to be secure and to provide for "roles based access". Officers will also have to authenticate against their devices before accessing its functionality, and then the relevant gateway.

It is now anticipated that this form of distributed user authentication may suffice to satisfy the needs of IDENT1, without the need for development of a separate access control regime.

It is also understood from the mobile information team that these gateways should become operational between September 2008, and March 2009.

RECOMMENDATION 2 -

That the IDENT1 engineering /security team work with Mobile Information engineers to better understand the architecture of the MI system and its security measures. IDENT1 engineers should also produce a document on the suitability of the system security so as to meet IDENT1 requirements, and the connectivity requirements for the provision of a national service. The Project Team to then report back to the Lantern Project Board.

[2] The vision statement set out by ACPO for UPSA /IAM is: 'The Police Service security architecture is to enable employees (and systems) to access the services, when needed, that they require under their basis of employment, whether access is via fixed, mobile or remote device, from either their 'home Force', 'other Force' systems or elsewhere, within security constraints.'

5. Re-Examination of Options 1-3

Option 1 End to End Managed service using Northrop Grumman and the Sagem Morpho RapID device.

As the interim solution, this was essentially a cut down version of Option 1, and has effectively been ruled out as being uneconomically viable for a relatively small number of devices, it may be considered as non viable for a wider, national solution.

This assertion is based on the fact that the major proportion of costs will escalate in direct proportion to the numbers of devices / users accessing the system and there is only a small opportunity to reduce some of the costs due to economies of scale..

Option 2 – 'Back end' kept with IDENT1, comms and Devices outsourced.

This was the preferred solution by the Lantern Project Board in June 07. Key advantages and disadvantages of staying with IDENT1 as the provider of the 'back end' are shown below.

Advantages of using IDENT1	Disadvantages of using IDENT1
Records already available for use, including demographics.	Tied to Northrop Grumman as supplier and their costing mechanisms
Able to use interfaces to other databases such as Immigration	Tied to NG's ability to meet development timetables
Device interfaces already established as part of pilot recommendations	No competition to drive down costs
	Need to meet stringent security requirements, the solution to which is very expensive.
	Lack of clarity as to what happens when IDENT1 contract comes to an end in 2013

When looking at the communications and devices being outsourced there are other distinct opportunities that should be considered.

At the project board in June 07 it was envisaged that the communications and devices would be provided through centrally negotiated contracts or catalogues that forces could 'call off' against. Such negotiated contracts and catalogues can provide cost savings through competitive tendering. However, it may also stifle innovation and could meet resistance from forces who want to do their 'own thing'. The expected benefits of the

competitive tendering are may be not realised due to the lack of buy in by forces.

The development of a catalogue of devices requires a stringent testing regime to be set up, and a robust, easily repeatable testing system to 'authorise' or 'kite mark' devices that are offered by suppliers for inclusion in the catalogue. This imposes a significant ongoing time and cost burden on the NPIA or a retained testing accreditor.

It may be more advantageous, if possible, to just 'authorise' the fingerprint sensor type, and provide the interface capability. This will shift device provision, maintenance, and servicing back to forces. It would enable forces to work with partners to provide their individual needs.

In terms of communications, this could also be left to individual forces to provide. The NPIA then only would need to provide the connection points to accommodate access via the different mediums, (SSL VPN, Wi-Fi, Broadband, GPRS, 3G, Edge, or Airwave). This could be as simple as a gateway sitting on the Criminal Justice Network.

The best way to achieve this approach would be through an OJEU process. However if due to time constraints, an OJEU process poses a significant hurdle this line of approach may present an avenue by which an OJEU process could be avoided.

<u>Option 3- Fingerprint Matching service and devices provided by independent companies. IDENT1 provides database with 'raw' fingerprint data.</u>

This option could also be achieved in the same way as options 1 and 2, a whole end to end service, or break each of the 3 parts into separate contracts.

This approach could provide a route to a very cost effective solution. However, it also could present a situation where certain user requirements cannot be met. Examples of this would be an inability to interrogate specialised databases on IDENT1, or to connect to the Borders and Immigration Agency database.

Although there are distinct disadvantages from moving away from IDENT1, there may be ways to overcome these. This option should not be dismissed out of hand.

It may be possible to conduct, over a short time frame, dialogue with selected suppliers (other than NG), to elicit what such a system could look like and obtain a rough estimate of costs. These would be a good comparison benchmark to measure the validity of any costs proposed by NG in the future.

An alternative approach would be to issue an OJEU notice, as the start of a procurement programme. An OJEU process is very time consuming in that much of the process is governed by time frames set out in legislation

and will take a minimum of 6 months to complete, nine months being more practical to get to award of contract status. If the project were to deliver in 18 months, this would only leave 9 months from contract award to full operational service. Such time frames would be achievable, but only with the correct commitment to internal funding and adequate resourcing.

One positive aspect of this approach is that the solution would be essentially independent of IDENT1, although still reliant upon the service for the initial fingerprint collection and updates.

RECOMMENDATION 3

Issue an OJEU notice, as soon as possible to initiate the tender process.

At present the key dates for the procurement are listed below.

Description	Target date
Redefine Procurement/Delivery approach and issue OJEU Notice	30 July 2008
Complete OJEU Procurement and Award Contract(s)	30 April 2009
Commence delivery of National capability to Forces	3RD Quarter 2009/2010
Complete and close down project	1st Quarter 2010/2011

6. Issues to be considered if Option 2 is taken forward.

If the project continues with using IDENT1 to provide the 'back end' matching service, then one key issue will be the sizing of the matching capacity, to meet demand.

NG have provided a document in July 2007, called "Lantern performance and scalability report", where it has analysed 84 days of transactions, to establish a use pattern from which they could determine the sizing requirements to the matchers to meet the sporadic demands of the front end users. Key to this sizing is the requirement imposed by the NPIA that the transactions should be no longer than 5 minutes.

The report shows that the enquiries are not uniform in their flow, and there are peaks of transactions all arriving at once. These bursts of

transactions, ultimately affect the ability of the system to process the enquiries in the required time constraint. Even so, their own figures show that this was being achieved for over [redacted] of the time.

It needs to be pointed out that there is currently no service level agreements in place to govern this, and during the recent CCN050 negotiations at the mention of imposing SLR/SLA's that NG baulked at this level of performance. NG stated that to guarantee this level of performance would require substantial investment in hardware which would be very expensive to implement.

It would now be prudent to instruct NG to repeat their performance and scalability report with a much larger data set – i.e. the last year of operations, to see if the same conclusions are reached. It would also be advisable to have them explain in simple terms what is needed to meet the SLR's and why.

RECOMMENDATION 4 Only if 'Option 2' is proceeded with

NG are instructed / requested as a matter of urgency, to revisit their 'Lantern Performance and Scalability report' and re-work using a years worth of transaction data, to provide a more refined model for future expansion.

Any future expansion to the matching capability, would be best served by having it implemented incrementally, rather than trying to guess up front the size it should be when the capacity and the numbers of users are unlikely to be known at the start. In short there is a requirement for the system to be scalable.

It is preferable to license users, rather than devices, as forces would then be better placed to examine the need for a particular person to have the ability to conduct fingerprint searches, rather than have a number of devices where the functionality is hardly used. User based licensing also fits hand in glove with having user level authentication.

Consideration needs to be given to costing mechanisms. It may be prudent to instigate user based costing as opposed to device based costing. This may encourage forces to consider who really needs access, and limit expansion so that it can be easier controlled.

The recovery of costs can also be spread over the remaining lifetime of the IDENT1 contract (due to expire in 2013).

7. The constants regardless of option chosen

There are a number of issues to be resolved regardless of the option that is chosen as the way forward. These can be summarised as:-

1. A suitable fingerprint sensor / device that meets user requirements, and an approval scheme for new devices or sensors.

2. User level of authentication.

3. PNC Warning flags.

4. A database matching capability to meet the expected demand and user requirement of the police service.

Of these, the most expensive to fulfil will be user level authentication, and service matcher sizing.

From the figures provided by NG in CCN050, due to the lack of granularity in the document, it is difficult to isolate particular costs just for matcher expansion.

However using CCN050 as a guideline, subtracting the cost of [redacted] devices [redacted][3] from the figures quoted for "MFR service increments", then adding on the other fixed and variable costs related to service expansion, the total for [redacted] devices / users is *indicated* to cost [redacted]. Extrapolating that cost to, say, [redacted] users, would *indicate* that the costs would be in the region of [redacted]. This seems an extraordinary amount for such a service, especially if those costs are to be recovered from forces over the residual lifetime of the IDENT1 contract.

We may, therefore, need to explore other ways of achieving this

8. Critical Success Factors

Critical to achieving the transition to a national service, it is necessary for the following to be achieved.

1. Clearly identified and agreed funding streams for both capital and revenue.
2. Complete 'buy in' at the outset from the Police Service. The Livescan Model achieved this via agreement at ACPO council.
3. Similar 'buy in' and commitment from senior NPIA management.
4. An agreed time frame to deliver the project taking into account the complexities of the procurement processes to be undertaken.
5. Adequate levels of resourcing for the project agreed at the outset..

9. Additional considerations and opportunities

If the decision is taken involves a step change to deliver the national solution, then it is important to keep the existing limited capability

[3] [redacted]

provided by the pilot, until such time as the national service is commenced, and is seamlessly transitioned

This would mean extending and protecting the current 'pilot' capability of 200 devices to at least December 2009. Currently the service is only guaranteed until mid December 2008.

If there is a demand from forces for additional pilot devices to be provided in the short term, the current 'pilot' capability has the potential, with a small, but limited risk, to expand the numbers of devices to 500, this being achieved without any need for central matcher or infrastructure increase.
Beyond this number of devices, the capacity issue is such that there is an increasing risk, according to NG's model, of regularly exceeding the 5 minute response target.

Any devices provided would have to be entirely funded by the forces themselves.

10. Control page

Distribution list

Recipient	Title	Location
For draft versions		
[redacted]	Project Manager	NKBH
Nick Deyes	Head of ICTS	NKBH
[redacted]	Head of Fingerprint projects	NKBH
For authorised versions, as above plus		
ACC Peter Goodman	Project SRO	Derbyshire
Lantern project board members	n/a	As per contact sheet

Change control

Version	Date	Authority	Evidence of approval	Record of change
0.1	3rd April 08	[redacted]		First draft
0.2	8 April 2008	[redacted]		Second Draft
0.3	9 April 2008	[redacted]		Third draft following review by C Wheeler

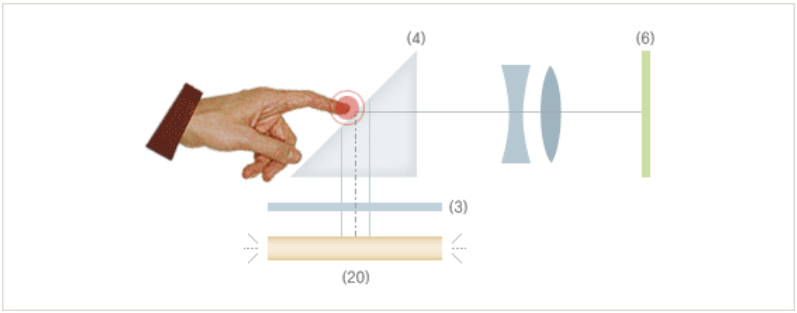
11. Annex A

This type of sensor can be called ‘capacitive’ or ‘semi-conductor’ It is very flat and can easily be built into a variety of devices such as:-

UPEK FIPS 201 Compliant
Silicon Fingerprint Sensor

Certified by GSA and FBI as
Single Fingerprint Capture Device

A prismatic optical fingerprint reader has a set of lens and prisms which it uses to catch the reflected light from the finger. These have to be a fixed distance apart so the devices are naturally bulky



A Thin film optical sensor is very much the same as the UPEK sensor above, except it is covered by a thin plastic film and has a light source which reflects light from the fingerprint back onto the sensor.

12. Annex B

Executive Summary from " Lantern Technical Options Paper- evaluation of fingerprint sensor technologies" by Ambika Suman

During the course of the Lantern Project there has been ongoing debate over the benefits of using capacitive sensor based devices in addition to optical based devices for fingerprint capture. To date there is currently no published data that can be used to inform this decision. Recently the NPIA has obtained ownership of Project Roman devices – these are similar to currently deployed Lantern units but capacitive based. Furthermore, the sensors used in them are the only type currently accepted as PIV certified, which is a reduced version of the appendix F compliance standard that is a mandatory requirement for sensors/devices used for searching police fingerprint systems.

The NPIA Biometrics team has been tasked with formulating a set of options for the Lantern project on how to perform an operational evaluation to compare optical and capacitive sensor technologies for police use by exploiting the availability of the optical based Lantern devices and the PIV certified capacitive based Project Roman mobile devices.

It is envisaged that the devices can be deployed operationally for side by side use with the Lantern units. For every individual stopped their fingerprints would be captured on both devices for searching on IDENT1, thereby providing opportunity to compare the search outputs and accuracy for the two technologies.

To evaluate the search performance of fingerprint images from currently deployed capacitive sensor and optical sensor technology it is recommended that the Lantern team perform operational tests during a period of dual operation of the devices for capture. Searching would be performed offline, however, searches on Lantern would continue as normal. In addition to this, a set of controlled tests would also performed with a group of volunteers (NPIA staff or Police officers) to assess the factors that cannot be observed or controlled in operation such as environmental factors, physical robustness of sensors, usability and so forth.

Finally, it is strongly recommended that in addition to testing the devices, a questionnaire or feedback exercise is conducted to note other observations that cannot be tested for. In particular, aspects around Usability such as the finger placement, pressure, sensor position, search time and response cannot be observed independently but are nonetheless important to the findings of the evaluation. The type of user feedback will vary across operational and controlled tests; therefore, feedback from an operational trial would provide the most information that is relevant and reflective of genuine end users' experience.