WHITEPAPER

How to Procure a Livescan System:

an Objective Guide for Decision-Makers

MorphoTrak
Contact us: (800) 601-6790 - www.morphotrak.com
113 South Columbus Street 4th Floor
Alexandria, Virginia U.S.A. 22314

SAFRAN
MorphoTrak

TABLE OF CONTENTS

1 Introduction and overview

This guide is intended to help you clearly define your assumptions and requirements in order to create an RFP (Request for Proposal) for one or more LiveScan fingerprint identification devices. This in turn will ensure that your expectations will be fulfilled and your implementation timeframes met.

The key to a successful procurement is for the vendor and the customer *at the outset* to come to a common understanding of the biometric capture problems and workflows to be solved. This has the added benefit of "protest-proofing" the RFP and subsequent purchase decision, by clearly defining your requirements up front. Any requirements that are insufficiently specified can incur additional costs due to contract change orders. Or, at the other end of the spectrum, you can end up purchasing capability that you don't actually need.

Whether you are sole sourcing your LiveScan identification solution, developing an RFP that will solicit multiple vendor responses, or enlisting a consultant for RFP development or assistance with the purchase decision, this document is intended to help ensure that the system you buy is the one you want, and the one the vendor plans on delivering.

2 Define your requirements

You've already decided that you need fast, accurate fingerprinting of subjects in critical booking situations, (either in the station or in the field), or for a background check submission or other civil application. It might seem like a simplistic statement, but it is essential to define your requirements so that your LiveScan vendor has an exact understanding of what you need.

The essential element of LiveScan is accurate, AFIS-quality fingerprint capture. Uses range from ruggedized cabinet solutions for jail booking to portable devices used during field bookings. Other uses include gang and drug raids, for sporting event security, during mass casualty events, in the Medical Examiner's office for identification of the deceased unknown, for immigration enforcement, or in commercial security applications.

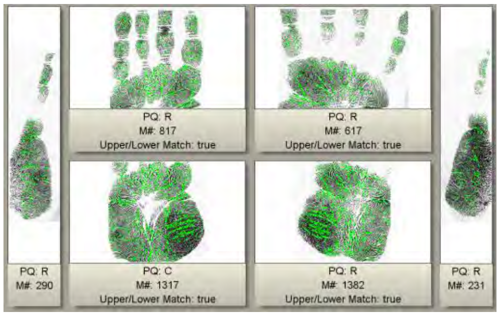
Before you issue an RFP, you need to thoroughly understand—and document—your essential capability and functionality requirements in terms of the identification problem to be solved.

Your agency likely has numerous stakeholders in the LiveScan procurement, and their priorities must be addressed.

Financial Managers need a system with no hidden costs. Vendors should clearly state their network or other infrastructure upgrade requirements. The solution should also allow reasonably easy technology refresh with a commitment to backward compatible capture devices.

The Information Technology department needs to protect the sensitive information within its databases and requires secure LiveScan devices that conform to the NIST and FBI EBTS standards.

Booking Officers require an easy-to-use device that can capture fingerprints, face (and optionally palms, scars/marks/tattoos, signature and iris) quickly, and submit for search. The device must be rugged to withstand a harsh booking environment, yet have no sharp edges that could cause harm, and have no easily-detached parts or cords that could be used as a weapon by an unruly subject.



Full Palm capture, including writer's palm

Officers in the field require an easy-to-use portable device that can capture fingerprints, face (and optionally palm and iris) quickly, submit for search, and alert them if the search results are positive without undue distraction or complexity. The device must be rugged, fit in a case, and function in a wide range of environments, including at night and in cold weather.

Court and Jail Personnel require both fixed and portable devices with fast response times, allowing them to quickly verify prisoner identity during transfer or release at both fixed and variable locations.

System Administrators require an integrated set of tools that allow them to manage remote users, devices, and software/firmware updates, view the current health of the system (hardware and software), and alert them to any potential problems.

The ID bureau manager looks at the big picture. He or she wants the best (fastest, most accurate) capture and submission workstation that will integrate seamlessly with the agency's Automated Fingerprint Identification System (AFIS). They want to future-proof their investment with a modular system that can be easily updated later with additional modalities such as palms, mugshot, DNA, voice, etc. They need the vendor to show a commitment to biometric standards developed by NIST, ANSI-INCITS, RCMP and FBI and show a commitment to interoperability and hardware independence.

It will be essential to address the needs of these various factions. You should solicit their input when documenting your requirements and evaluating responses, so you can come to the most informed purchase decision.

Developing a relationship with LiveScan vendors early in the process will help you gain an understanding of their offerings. This in turn will help you define a solution that will meet your needs. You can take advantage of vendor expertise throughout the process by doing the following:

Consider releasing a Request for Information (RFI) to vendors. Response documents typically do not exceed 10 pages, and will help you understand their current offerings. In addition, a vendor's response to an RFI can be an indication of their willingness to work with you.

Draw up a draft Request for Proposal (RFP) and send it to vendors for comments. Their responses will clarify potential issues or ambiguities in your RFP that could impact your agency.

Use standard vocabulary in the biometrics requirements. Such terminology can be found in ISO SC37 Harmonized Biometric Vocabulary (Current Version Document 2 Version 12 - dated 2009-09-16).

When you release the RFP, be sure to **include a period when vendors may ask clarification questions**. (And be sure you answer them in a timely manner.) You may also want to schedule an on-site facility tour and/or a live vendor demo and question and answer session.

2.1 Understand & document the problems to solve

You must define your LiveScan identification needs to really get the solution you want—and conversely, to ensure that the vendor does not over-configure their solution. Will you be performing jail bookings, or enrolling applicants for a background check, or both? Will you be identifying unknown persons or verifying a claimed identity? Will you want to get explicit notification of individuals on a watch list? Do you have multiple workflows, each capturing a slightly different dataset? Might you wish to capture face, palms, scars marks and tattoos, or signature, or add a new biometric to an existing record without re-booking? Do you anticipate situations where you have limited or no connectivity and require *local* searches?

Local city/county AFIS vs. State AFIS vs. FBI NGI (Next Generation Identification): Which AFIS database(s) does your agency wish to search? Most agencies want to search their local AFIS for positive identification (for example to know if a booking subject is giving a false name). You need to specify how you wish to interact with these systems and the type and format of data that will be exchanged, as well as the order of search and how results from multiple databases should be returned. Will the vendor allow responses to be customized according to your agency's requirements?

Background checks: In states that do not have a separate background check service, background check enrollments are performed at the local Police or Sheriff level. Does your agency require this capability?

Sex offender enrollment: The Sex Offender Registration and Notification Act (SORNA) specifies that registered sex offenders be booked with palms and answer specific questions. Does your agency require the sex offender booking workflow options?

One-to-one search verification: LiveScan can be very useful for quickly answering the question "is this person who he says he is?" and is used to verify the identity of an individual, such as confirming the identity of a prisoner prior to release from jail. One-to-one searches are less processor-intensive and can return a definitive match/no-match response more quickly than a one-to-many search.

One-to-few watch list check: This approach is typically employed in situations where your needs may include times when there is no connectivity to a back-end system possible. This answers the question "is this person dangerous or wanted?" based on a subset database of "persons of interest" searched on a local device rather than the back end system. Another scenario this might be employed where, even with back-end connectivity, the target system is near maximum capacity and a reduced search set in the form of a watch list is employed to minimize processing load on the target system. This approach would be used to determine if an unknown individual is on a watch list and should therefore be detained for further questioning but may not identify the individual if known to the agency but not on the watch list.

One-to-many search identification: Most typically used in a booking environment, this workflow answers the question “who is this person?” and is used to identify an unknown individual, such as someone who is giving a false name or who cannot produce a valid ID. Because each search print is compared against the entire database, these searches could take longer or require more processing power.

If you do not clearly state the problems you need to solve, or if you impose a “how to solve” in your RFI/RFP, vendors may propose an artificially inexpensive approach instead of the one that actually meets your needs. Conversely, the solution may have unnecessary costs as vendors may over-engineer the system, either of their own accord or to meet an imposed solution, without adding value to solving the problem.

2.2 List your essential livescan capture and identification requirements

In addition to documenting your high-level process-related requirements, it is important that you clearly define your requirements in a number of additional categories.

Device form factor: At the most basic level, one of your first decisions should be whether you want a ruggedized cabinet, a desktop system, or a portable configuration. There are advantages to each approach and will depend on where and how you want to use the device.

500 vs 1000 ppi: Does your agency require 1000 ppi image capture? Keep in mind that 1000 ppi images are four times “larger” than 500 ppi images, so there are network bandwidth and speed considerations. If you are capturing 500 ppi images now but wish to upgrade to 1000 ppi in the future, how easy or difficult is it to make the upgrade?

Data capture: In addition to fingerprints, consider what other data you want the LiveScan identification devices to capture. Do you need to also capture palms? Facial and/or scars/marks/tattoo? Iris images? What do you intend to do with the images?

- **Palms:** The FBI NGI system now accepts palms. But because of their large image size, palm capture may put a burden on your system’s memory (see “Performance” below).

Livescan cabinet

- **Face:** Does your system need to capture face/mugshot images? You should specify that photo capture conforms to current FBI standards (see section 2.3 below). But avoid specifying exact camera models, or you will risk requesting an item that is no longer available from the industry. Additionally, some LiveScans provide an auto face finding feature; is this a requirement for you?

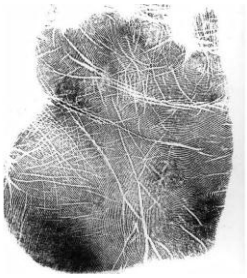
- **Signature**: Does your agency's current workflow call for capturing officers' and/or subjects' signatures? You will need to include a signature pad and stylus in your requirements.

- **Scars, marks and tattoos:** How will you capture scars/marks/tattoos? How do you intend to use them? You must specify if you require an interface to an existing mugshot system.

- **Iris:** Do you require a camera that can capture the subjects' iris images? Do you need capture only, or iris match results?

- **DNA:** Should the LiveScan device accommodate a DNA workflow? Twenty-six states now have state laws to collect DNA samples from people arrested for felonies. If your agency is in one of those 26 states, you will save time and money by including this workflow with the LiveScan. Following the June 2013 Supreme Court decision in Maryland *vs*. King, in which they ruled that police can collect DNA from people arrested but not yet convicted of serious crimes, it is possible that more states will implement such laws. Does the vendor make it easy for your agency to update the charge lists which trigger a DNA collection?

Adding additional biometrics: If you decide later that you want to capture any of the additional biometrics listed above, such as palm, face or signature, how easy is it to upgrade the LiveScan device with the required hardware? Will it also require a full software upgrade, or can a system administrator make a simple change to enable the capability? Does the vendor offer a workflow manager which allows you to add these to an existing booking?



Palm capture

Hardware and peripherals: What other hardware will be attached to the LiveScan device — for example, a barcode reader or mag stripe reader? Does the device need to also support a tenprint inked card scanner? Will you need an Appendix F certified card printer, and must the printer support multiple card formats?

Ease of use, user experience: How important to you is ease of use? Do you require intuitive GUIs and workflows? Features that can contribute to ease of use include live display of the captured image; automatic advance to the next capture step; AFIS quality evaluation; flagging of missing or out-of-sequence prints; rescan and override capability; pick lists, context sensitive or type-ahead descriptor fields; descriptor field validation; etc. The more features you specify, the more confident you will be that the LiveScan will meet your needs. However, over-specifying non-essential capability can lead to increased costs.

Workflows: What are your requirements for capture time to complete a workflow? Do you require an offline training workflow? Will you have the ability to add more workflows later, such as civil, booking, sex offender, etc.? How easy or difficult will that be (see "Configurability" below)?

Security: What are your data security requirements? Do you need to be able to define separate privileges/abilities for users and administrators? Do you require a multi-factor login (e.g. password and fingerprint)?

Connection to AFIS: In addition to one or more types of frontend LiveScan capture devices, your identification system will need a connection to AFIS system(s). The LiveScan vendor should therefore describe the AFIS connectivity *and* how the LiveScan will handle images that it submits but are rejected by the AFIS.

Additional considerations for the AFIS interface may include the ability to synchronize with the multiple local/state or FBI AFIS through an external interface and communications protocol based on EFTS/NIST formatted transactions or XML formatted transactions.

RMS or JMS interface: Does your agency have a Record Management System (RMS) or Jail Management System (JMS) separate from the AFIS/CCH? If yes, do you want the LiveScan to interface with the RMS or JMS to eliminate duplicate data entry?

Network connectivity: How will LiveScan devices communicate to the backend? If network connectivity is lost, how are transmission errors handled? A well designed solution will be designed to use TCP/IP transparently over the agency's data network. Note that the agency, not the vendor, is typically responsible for the network, connectivity between the edge devices and back end, and any monthly access fees.

Optional gateway/server: Will you need a dedicated store and forward gateway/server? An optional separate server can provide management functions and increased capability in your LiveScan system *without* requiring extensive (or any) modifications to the existing back-end system. This approach also affords a single point of contact to your AFIS which can simplify implementation. The gateway/server can also provide connectivity management and advanced business processes for interface to multiple ABIS with escalated or parallel search, CCH, RMS, photo image, and other databases.

System administration and monitoring: System administrators and IT professionals must be able to easily access the LiveScan system monitoring and transaction information they require. The LiveScan system should allow you to view transaction queues, manage all connected devices, monitor system performance, and push software loads. What are your requirements for file retention and/or automatic deletion of records?

Configurability: Does the LiveScan provide the ability to add new workflows later, or change existing workflows? Will you have the ability to add data fields? How easy is it to update charge tables/offense codes?

Performance: Is the CPU fast and powerful enough to capture 1000 ppi images quickly? Palm images are approximately 3MB each; if you require palm capture, can the CPU accommodate the added load? Do you require local matching on the device? That will put an additional burden on the CPU.

Availability and downtime: Requirements for availability specify the maximum unscheduled downtime for the system. It is important that you define exactly what you mean by "downtime". Is the system "down" if any component fails, or must all fail? Does your definition of downtime apply only to the backend matching system, or does it include the capture devices?

Finally, when specifying availability, keep in mind the limitations of your own network infrastructure. Uptime and availability are not synonymous. A system can be up, but not available, as in the case of a network outage. When calculating system uptime or availability, the LiveScan vendor cannot be held accountable for network failures. The network must be able to support your desired availability.

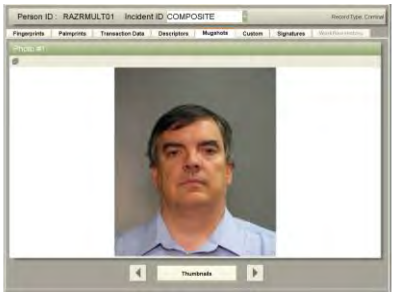
24-hour support center: How important to you is it that the vendor maintain a 24-hour center where you can talk to a human who will trouble-shoot your problem regardless of the time of day? You must specify the hours you expect support to be available—and what type of support will be provided.

Price: Don't fall into the trap of thinking that all LiveScan identification solutions are alike and that the only differentiator is price. Also don't fall into the trap of looking only at device price without considering associated peripherals or gateway servers. With today's fingerprint technology, you truly do get what you pay for! If you place too much emphasis on the unit price of the capture device, you run the risk of purchasing an inferior system and incurring costly add-ons to get the system you actually wanted. Because this is such an important topic, pricing evaluation is discussed in greater detail in its own section of this document.

2.3 Be aware of livescan identification standards

You will want your LiveScan identification system to conform to the latest ANSI/NIST ITL and FBI EBTS industry standards. Information captured, compiled and formatted in accordance with and compliant with the target system's implementation of the ANSI/NIST-ITL (described below) can be transmitted and seamlessly exchanged.

The ANSI/NIST ITL specification is defined by the National Institute of Standards & Technology and is updated at least every five years. The current specification is ANSI/NIST ITL 1-2011. This update to the NIST biometric data standard adds DNA, footmarks and enhanced fingerprint descriptions for marking extended feature sets.[1]



Person ID : RAZRMULT01 Incident ID COMPOSITE Record Type: Criminal

Mugshot capture

If you require mugshot capture, the device should conform to the standards outlined in the NIST Best Practices Recommendations for Capture of Mugshots, Version 2.0. Included in the standards are recommendations for pose, centering, three-point lighting, background, etc., that will yield uniform images for improved search/match results.

The FBI Criminal Justice Information Services Division also has a defined specification, known as EBTS (Electronic Biometric Transmission Specification). Though fingerprints will continue to be the FBI's primary mode of identification for the near future, the scope of the EBTS has been expanded over previous versions to include additional biometric modalities (e.g., palmprint, facial, DNA and iris) in recognition of the rapidly developing biometric identification industry. Integrating biometric data in accordance with the ANSI/NIST standard, the FBI EBTS provides a description of all requests and responses

[1] http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910136

associated with electronic fingerprint and other biometric identification services.[2] The current version is EBTS v9.1 XML IEPO.

If you are a state agency and want your system to connect with FBI NGI (Next Generation Identification), it must conform to EBTS and ANSI/NIST-ITL. But beware of fingerprint standards that are not relevant to AFIS or forensics. Including the non-relevant standards listed in the table below leads to unnecessary confusion or may introduce mutually exclusive requirements.

Non-AFIS Fingerprint Standards. *Including these standards in your LiveScan requirements will lead to confusion.*

INCITS number	ISO/IEC number	Description
INCITS 377-2004	ISO/IEC 19794-3	Finger Pattern Based Interchange Format
INCITS 398-2004	ISO/IEC 19785	CBEFF (Common Biometric Exchange Formats Framework)

ANSI INCITS 377 - Finger Pattern Data Interchange Format
Non-forensic non-minutiae matching used in door-lock access control devices by a single vendor, and is not used in LiveScan or AFIS systems.

ANSI INCITS 398 - CBEFF
Promotes interoperability by allowing different vendors' biometric devices and applications to exchange biometric information[3].This specification is not used in LiveScan or AFIS systems.

You should clearly identify which standards are relevant and that the system must adhere to, and make them available to vendors for reference. A link to a website where they can download the standards is sufficient.

3 First things first

The majority of this document describes numerous factors you need to consider when defining and selecting your LiveScan solution. Yet there are a few things that your agency needs to do *before* you go very far down the livescan procurement road. We're discussing them last, but you should actually do them first.

Determine how you will pay for it. Will it be funded from your budget? A special tax or assessment? A state or federal grant?

Determine where you will put it. If buying a LiveScan cabinet configuration, do you have the necessary floorspace? If buying a desktop system, do you have the desk? In all cases, do you have the electrical and network connections in place?

Register with your submission agency. Whether law enforcement or civil, each agency that accepts electronic fingerprint records has its submission requirements, and may require you to register. Section 2.1 above regarding workflows and agency submissions assumes that you have completed this essential step.

[2] FBI Biometric Center of Excellence: https://www.fbibiospecs.org/ebts.html
[3] http://en.wikipedia.org/wiki/CBEFF

4 Evaluating vendor responses

You will have an easier time evaluating the vendor responses if your requirements are listed in a way that can be **measured** and **met**. You must specify your needs and wants clearly so that you have a basis of comparison of proposals. This starts with requirements for organization of the proposal, and carries on to specifying which of your requirements are mandatory and which are optional or nice to have. You can go even further, and rank the mandatory requirements by assigning a point value to the answer that corresponds to its relative importance.

Include in your RFP the standard you will use to determine if an answer is good, poor, or outstanding, and what point score you will assign to each. Some criteria include compliance, completeness, understanding of the requirement, standard product feature already implemented and deployed to other customers and whether a response goes beyond what is required, thereby supplying extra value.

There are certain contractual requirements that may seem like a good idea, but that can cause you to make a decision you could come to regret, or cause implementation delays. Some of these are:

Capture time and image quality: your goal is for AFIS to accept your livescanned images. You need to understand the relationship among capture time, image quality, and resultant search accuracy. Placing too much emphasis on capture speed in your requirements may result in more images being rejected by the receiving AFIS.

Early delivery: if you award evaluation points for early system delivery, vendors will be tempted to try to earn the extra points. They then may or may not be able to deliver on their promise, resulting in unwanted delays. An alternative that can bring the desired outcome is to structure the scoring so that you award bonuses or penalties for delivery after contract award, but not for claims made in the proposal.

ADA Section 508 compliance: your state may require that you flow down Federal requirements from the Americans with Disabilities Act section 508 regarding information technology accessibility. Some of the provisions of this statute (for example, those in §1194.21 pertaining to Software Applications and Operating Systems) are not always relevant to LiveScan, and can cause delays while they are negotiated out of your purchase contract.

4.1 Pricing

The main objective of the foregoing sections, where we have emphasized the necessity of clearly defining your requirements, is to enable you to directly compare vendors’ offerings on an apples-to-apples basis. This is most effectively done through your pricing tables.

You should beware of a proposal that offers a “bare bones” system that does not meet your specified needs. You may be seduced by the low price, then find that it requires extensive (and expensive) change orders to fully satisfy your requirements. After-the-fact change orders can be used not only to overcome the problem of poorly defined requirements, but also to mislead clients with a seemingly low price.

With this in mind, you should structure your pricing tables (or require that the vendor structure them) so that they clearly show the following:

Basic System Cost: Pricing tables should clearly separate the optional and mandatory requirements.

Warranty: The vendor should clearly specify what type of warranty is offered. Will they send a repair technician, or send spare parts that you must install yourselves? What is the length of warranty coverage? Is it 3-6 months, 9 months, or 12 months? Does warranty include state submission updates and software patches and fixes?

Maintenance: What are the follow-on maintenance costs? How many years of maintenance are offered? The pricing tables should clearly state the warranty period and cost for maintenance afterward.

Training: What type and level of training is offered? Is it on-site? For how many users/operators? Is it a comprehensive training program, or a train-the-trainer? Is there a separate course for system administrators? Do they offer follow-on training for new personnel?

Price should be a separate evaluation component of the proposal, but not the deciding factor. It is better that pricing count for a certain percentage of the evaluation (ideally no more than 15 to 20%).This is preferable to a complicated formula in which higher-priced offerings are marked down by a weighted percentage. A less complicated and subjective evaluation formula also reduces the likelihood of protests from losing vendors.

Finally, you can make a more impartial purchasing decision if you are not influenced from the outset by the price. Specify that vendors provide pricing in a separate sealed section of the proposal, and that no mention of pricing be contained in the body of the proposal. Best practices mandate that no one in your agency open the sealed price until after all proposals have been graded.

4.2 Additional evaluation criteria and other intangibles

If you have followed all the advice above, you should be able to quickly evaluate the compliant vendor proposals. But before you make your decision, there are a couple of other aspects of the vendors' offerings that you should take into account. The items below cover not only vendors' technology, but also their methodologies and their relationship with their customers.

Customer references can be another factor that will tell you a lot about your vendor. Is your selected vendor well established in the industry with a proven track record of AFIS-quality LiveScan solutions and image capture devices, or are they a recent start-up? You should ask for references that are similar in size and scope (number of devices, throughput and response time) to your desired LiveScan system. But also consider requiring references from your vendors' long-standing customers as well as recent installations. This will tell you not only that they can acquire and keep customers for long periods, but also that they continue to add new customers.

Does the Vendor conduct a yearly **Customer Satisfaction Survey**? Ask to see the percentage of respondents that identified themselves as either Satisfied or Very Satisfied with the service support provided during the year.

Does the vendor not only **keep up with emerging standards**, but actually participate in the bodies that define the standards? Active participation in the ANSI National Institute of Technologies (NIST) and the International Association for Identification (IAI) should be a mandatory requirement for your chosen LiveScan vendor. Other biometric and identification associations and interest groups include the International Biometrics & Identification Association (IBIA), Security Industry Association (SIA) and Biometric Consortium.

How the vendor handles your project once the contract is signed is another important consideration. For large-scale LiveScan implementations, they should use a defined **Program Management** process that adheres to the standards of the Project Management Institute (PMI) or other body. The PMI standards are outlined in the PMBOK Guide (Book of Knowledge). The PRINCE2 method is the standard in the UK and other countries.

Software development is another area you can use to evaluate a vendor’s capabilities. Do they have a defined process for software enhancements? How do suggested improvements in user interface, workflow, or hardware become part of the product? Is there a defined product roadmap? Do they have regular software releases? Do they release standard software, or does each customer have a unique software package? Are improvements developed with real world input from users, or by software developers with no identification background who deliver what they think the customer wants?

To make sure that both you and the vendor are in agreement about the system that they will deliver, the vendor should deliver a **Requirements Document** that describes the features and functions of the system, as well as the timing of the deliveries. This will correct any misunderstandings before they happen and resolve potential disconnects among the RFP, the proposal, and the signed contract. You and the vendor should both sign off on the document, which then becomes part of the system deliverables package.

Once your system is delivered and installed, it must be kept in good working order. Consider the following points before you make a purchase decision:

- Does the vendor have a documented problem management philosophy to resolve system issues before they are likely to occur through proactive routine support and maintenance functions? When escalation is required, does the vendor follow strict escalation procedures dictated by the level of problem severity? Does the Escalation procedure include the direct involvement of vendor management in an ordered, ascending line of responsibility?

- What type of service reporting does the vendor offer? Can they provide you examples of monthly reports generated from their internal tracking system? Does it integrate customer service call tracking with automatic technical escalations as well as with internal Quality and Engineering departments? This approach ensures immediate visibility to all reported issues. Do they automatically record all warranty service activity for the agency and track in an integrated tracking system? Monthly reports should show all service activity conducted during the previous 30 day period including:

  - All service activity requested during a 30 day period
  - Date and time of request for service
  - Problem description
  - Details on problem diagnosis and troubleshooting actions
  - Problem resolution

- Does the Vendor have a documented plan for Spare Parts Management? Rather than simply forwarding the service request on to the part manufacturer, does the Vendor offer a total support ownership approach for hardware service? To minimize unscheduled downtime, a vendor should have an established spare parts inventory management system designed to have the right part or unit at the right location at the right time. The Vendor should have the infrastructure in place to offer a comprehensive parts support approach to your agency. Has the vendor identified a critical spare inventory list of parts that will be maintained for ready availability to support your agency to ensure strict compliance with your requirement for replacement within 24 hours of determination?
- How many full-time customer service engineers does the vendor have in your county? In your state? That is, does the vendor really have the infrastructure in your state to support you? Is there a commitment to be on-site within 4 hours, or only within 24 hours? Can you afford to be down that long?

5 Summary and conclusion

There are now numerous vendors who offer LiveScan capture devices and their associated systems for identification. Determining which one will give you the best possible system that meets your needs doesn’t have to be a coin-toss.

This document should have given you some guidelines to help you define your requirements. If you clearly specify what capabilities are mandatory and which are optional; if you define the system under which you will rate proposals; and if you make sure that pricing tables are as unambiguous as possible, you will be in a better position to make a purchase decision for your agency that you will be happy with for the next decade.

Acronyms and Abbreviations

ADA	Americans with Disabilities Act
AFIS	Automated Fingerprint Identification System
ANSI	American National Standards Institute
CBEFF	Common Biometric Exchange Formats Framework
COTS	Commercial Off-The-Shelf
CCH	Computerized Criminal History
EBTS	Electronic Biometric Transmission Specification
GUI	Graphical User Interface
IAFIS	Integrated Automated Fingerprint Identification System
IAI	International Association for Identification
IBIA	International Biometrics & Identification Association
IEPO	Internal End Point Object
INCITS	InterNational Committee for Information Technology Standards
ITL	Information Technology Laboratory
JMS	Jail Management System
NGI	Next Generation Identification
NIST	National Institute of Standards & Technology
PMBOK	Project Management Book of Knowledge
PMI	Project Management Institute
Ppi	Pixels per inch
PRINCE2	PRojects IN Controlled Environments
RCMP	Royal Canadian Mounted Police
RFI	Request for Information
RFP	Request for Proposal
RMS	Record Management System
SIA	Security Industry Association
XML	eXtensible Markup Language

SAFRAN

Morpho

for more information:

MorphoTrak Inc.
Corporate Headquarters
113 South Columbus Street, 4th Floor
Alexandria, Virginia U.S.A. 22314
Toll-Free: (800) 601-6790
Phone: (703) 797.2600
Fax: (703) 706.9549