# BAYONET DEVICES PROJECT TBH

ENG 4000 – Capstone 2020: Gate 1 Review

## Bayonet Devices

**Created by:**

Hossam EL-Shebiny - 214163240

Daniel Tarasio - 214354419

Zeenia Akram - 213657093

Brandon Loy - 214233928

Dennis Bragilevsky - 214230445

Dalan Shakaj - 214206049

Sam Guraya- 214268916

Josh Abraham - 214334643

# ABSTRACT

**RE: NSPA Supply Opportunity No. 20LDS067**

**Tactical Handheld Multi-Modal Biometric Data Capture, Storage and Matching Device**

Here at Bayonet Devices, we believe that collecting a person of interest’s biometric information is critical, not only for national security but also for the general public’s safety in various scenarios. This can include checking in at an airport, registering for voting, or in more critical situations like a NATO support mission. Our device line *Tactical Biometric Handheld (TBH)* will be used to meet the growing need for biometric authentication. The agents that will use our devices will have a lot of functionality right at their fingertips in a sleek, easy-to-use, which will deliver excellent performance by taking precise, high resolution biometric scans in a quick and efficient fashion. Our device will perform biometric scans and allow for the creation and verification of profiles of a person of interest or public user. This process will be delivered via an intuitive user interface, allowing for easy training, and within a variety of situations. Our product also offers a full end-to-end experience for government bodies, including the physical device, the on-board software, and cloud integration matching systems that can be integrated with current NATO biometric cloud systems.

Contents

[Problem Statement 3](#_Toc55131033)

[Key Objectives 3](#_Toc55131034)

[Shortlist of Key Requirements 4](#_Toc55148886)

[Why was the project created? 9](#_Toc55131035)

[Stakeholders 10](#_Toc55131036)

[Original Project Stakeholder - NATO 10](#_Toc55131037)

[New Project Stakeholder - TSA 10](#_Toc55131038)

[Identifying Stakeholders 11](#_Toc55131039)

[Other Potential Stakeholders in the Future 12](#_Toc55131051)

[Our Team 14](#_Toc55131057)

[Personal Project Motivators 14](#_Toc55131058)

[Team Skills 15](#_Toc55131059)

[Gaps in Team Skills & Solutions 16](#_Toc55131060)

[Survey of Solutions 17](#_Toc55131061)

[Review of Requirements 18](#_Toc55131062)

[Out of Scope Requirements 18](#_Toc55131063)

[Challenging Requirements 20](#_Toc55131064)

[Poorly Defined Requirements 20](#_Toc55131065)

[Areas of Non-compliance 20](#_Toc55131066)

[Preliminary Verification Approach 20](#_Toc55131067)

[Full Table of Requirements 21](#_Full_Table_of)

[Works Cited 3](#_Works_Cited)

# Problem Statement

Biometric data is becoming the de facto standard in reliable security authentication due to its ease of use for the user and difficulty to impersonate for third parties. Even though many companies have attempted to address the growing interest in this technology, there continues to be no end-to-end biometric scanning system with matching capabilities that offers a fully secure storage environment. These systems are often expensive, and do not allow for flexible hardware options for increased lifespan and technology support. Many government bodies and organizations globally are looking into integrating biometric systems to strengthen security and reduce fraudulent activity. They have implemented several roadmaps but due to their large scale, the development is slow, incremental, and extremely costly. The objective of this project is to produce a viable alternative to currently available models for use within a myriad of government bodies. By leveraging advances in biometric hardware, and the use of secure cloud computing environments, our product will be able to address the growing need for a secure, closed loop, and extendable, biometric authentication system.

# Key Objectives

Within this project there are multiple critical factors that indicate whether our project would be considered a success. The overall objective of this project is to create an end-to-end biometric data capture system. This includes the creation of a multi-modal biometric scanning apparatus capable of creating user profiles with information gathered from fingerprint and facial recognition data. The next aspect of the end-to-end system will be to create a user-friendly application that communicates with the hardware apparatus for both the creation of profiles, and user identification. Additionally, the data captured from the application will be securely transmitted to a secure cloud environment and can integrate with pre-existing biometric data on the cloud environment. Finally, this system needs to be able to support 1-to-1 matching of fingerprint scans and facial recognition to profiles stored with the secure cloud database. Overall, creating this full end-to-end experience will alleviate traffic when using the device, increase the amount of biometric data sent to the database, all within a secure manner that meets stringent biometric data standards.

# Shortlist of Key Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID** | **Description** | **Source** | **Comment/Justification** | **Subsystem** | **Validation timing** | **Validation Approach** |
| **HW-FUNC-03** | The device storage shall be able to hold all software, including Android OS, Drivers for sensor devices and App. | NSPA Supply Opportunity No. 20LDS067 Document | Device should be able to hold all necessary software to perform its intended functionality. | Storage | Preliminary Design Phase | Check android device storage capacity and size of all software package file sizes |
| **HW-FUNC-06** | Hardware shall be capable of running android. | NSPA Supply Opportunity No. 20LDS067 Document | As per request. | Android Device | Preliminary Design Phase | Check device compatibility with android software. |
| **HW-FUNC-08** | The device shall be equipped with a NIR-sensitive camera. | <https://arxiv.org/pdf/2008.08220v1.pdf> | NIR-sensitive cameras are optimized in performance in the NIR range. This is required for capturing a high-resolution image of the iris. | Iris Scanner Module | Preliminary Design Phase | Confirm the camera is NIR sensitive before purchasing it. |
| **HW-IF-05** | The device shall be able to be charged while connected to the sensors | Hardware Team | Required to charge the battery without disassembling the product | Power Delivery | Preliminary Design Phase | The wiring between the device and the charging port shall be on their own breakout circuit using the 5V and ground pins located on the phone |
| **HW-PERF-01** | The device shall use 2 batteries (1 extra easily replaceable battery) that will provide power at 3.7V to the android phone and the sensor device(s). | NSPA Supply Opportunity No. 20LDS067 Document | Easy swap of batteries to prolong device use time in a critical situation faced by support teams | Power Delivery | Preliminary Design Phase | Test battery voltages and battery health. |
| **HW-PERF-03** | The batteries of the device shall be able to charge using 1 USB adapter with dual supply voltage (110V/220V). | NSPA Supply Opportunity No. 20LDS067 Document | Ease of use, less cables to carry for charging the device or its batteries. | Power Delivery | Preliminary Design Phase | Hardware design in PDR |
| **SW-BKND-01** | The backend system shall store information received from device in encrypted fashion. | NSPA Supply Opportunity No. 20LDS067 Document | Required for FBI compliance for EBTS standards (NGI-DOC-01862-1.1) | Backend Software | Critical Design Phase | Data will be encrypted using encryption libraries. |
| **SW-BKND-02** | The backend system shall have the ability to control which Android biometric devices can access the app. | Software Team | There will be more than one device that will be capturing and performing biometric matching at a time | Backend Software | After the biometric capture and  matching app is made | Test if more than one onboarded android device can send and receive information to the backend system |
| **SW-BKND-03** | The backend shall have the ability to enable/disable features on the Android app. | Software Team | Required for security purposes and lock out unknown users in case of device loss or theft. | Backend Software | Critical Design Review | Implementing flags to enable/disable features |
| **SW-FUNC-01** | The software shall be android compatible. | NSPA Supply Opportunity No. 20LDS067 Document | As per request. | Application Software | Preliminary Design Phase | Develop android app for the device and integrate with backend/online database. |
| **SW-FUNC-02** | The android app shall be capable of sending and receiving profiles from the backend database. | NSPA Supply Opportunity No. 20LDS067 Document | Required for functionality. | Android Device | Preliminary Design Phase | Send test profiles and compare to original version. |
| **SW-FUNC-04** | The database shall be backwards compatible with existing data stored in the HART database. | Software Team | Required for stakeholder purposes | Backend Software | Preliminary Design Phase | The same organization and parameters shall be used. |
| **SW-FUNC-05** | The profile storage system shall be able to store user information associated with a specific user (i.e. listing name, location, reason for entering, date of birth, etc.). | Software Team | Required for stakeholder purposes | Backend Software | Preliminary Design Phase | Parameters shall be added and linked to profiles |
| **SW-FUNC-06** | The biometric information stored in database shall be accessible by users and devices with credible/correct IAM (identity and access management) roles. | Software Team | Managing access to data is important. Roles with certain permissions should be created to limit and give access to devices and users. | Backend Software | Accessibility can be  tested during PDR  project phase | Test to see if IAM roles without  correct permissions can access  data |
| **SW-FUNC-09** | The backend system shall use AWS Lambda to send user information to an endpoint to create the user profile. | Software Team | Lambda is a serverless service provided by AWS. It allows for simple integration and setup. Apps also need a way to tell the backend system to create a profile which will be done by calling this endpoint | Backend Software | Preliminary Design Phase | Create lambda endpoint, using AWS console. Call lambda through API calls to see if profiles can be  created |
| **SW-FUNC-10** | Employees creating profiles and doing biometric scanning shall get authentication access (login) through backend system to perform task. | Software Team | Required for security purposes | Backend Software | Critical Design Review | Proper login credentials shall be distributed to authorized users |
| **SW-FUNC-17** | The on-board application shall transmit data according to the Electronic Biometric Transmission Specification (EBTS standard) | Software Team | Required for any government level biometric transmission. | Application Software | Critical Design Review | The generated format will match the specification documentation, and examples given. |
| **SW-FUNC-18** | The on-board system will be able to encrypt all data to meet government standard, AES encryption. | Software Team | Required for security compliance. | Application Software | Critical Design Review | Using pre-made encryption software that meet the standards of the regulatory body and all stakeholders. |
| **SW-FUNC-24** | The device shall perform 1:1 matching based on the search field of user id. | <https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf> | 1:1 matching is a core requirement from stakeholders | Backend Software | Critical Design Review | Research and implementation will be done to create a matching algorithm based off current biometric research. |
| **SW-FUNC-26** | Matching shall be done using at least two different biometric data (face photo, and fingerprint). | <https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf> | Required that the system developed is multimodal, and so having at least two biometric readings is essential. | Backend Software | Critical Design Review | Multiple matching algorithms with confidence intervals will be developed, to ensure there is a high degree of confidence of a match, no match scenario. |
| **SW-FUNC-28** | The system shall be able to complete a 1:1 matching verification process in under 30 seconds. | Software Team | Required within the TSA project outline. | Backend Software | Critical Design Review | Using lightweight and fast APIs to ensure fast responses, and the creation of multiple endpoints for matching to improve multi-user speeds. |
| **SW-FUNC-31** | The software shall be capable of presentation attack detection including detecting printed images and textured contact lenses. | NSPA Supply Opportunity No. 20LDS067 Document | Given the nature of our project, security is a crucial element that cannot be compromised. Thus, it is vital that the iris recognition software is spoof resistant. | Iris Scanner Module | Testing Phase | Once the iris recognition software is ready, we will test whether the software is able to detect when a printed image or textured lens is presented. |

# Why was the project created?

The NATO Support and Procurement Agency (NSPA) has shown interest in the creation of a handheld multi-modal biometric scanning and matching device for use within military-like operational environments. This contract request is intended as a replacement for the previous handheld device BioSled II, by Northrop Grumman. The intent of this contract is to create a faster, more accurate biometric scanning system, that handles the shortcomings of the previous device. These shortcomings include: a lack of software reliability, poor user experience, and device performance. The BioSled II product was later terminated, and so this project is also motivated by the lack of supply of biometric devices for governmental use.

Additionally, there is a separate contract being undertaken by Northrop Grumman to create the Homeland Advanced Recognition Technology System (HART) as a replacement of the legacy Automated Biometric Identification System (IDENT). This system will be the new main storage location for biometric data, and processing used by NATO, and various other government bodies. With this new cloud system, the aim of NSPA’s contract is to also allow for the new biometric device to be able to interact with this new system, as well as allowing for a higher capacity of daily transfers from a single device as biometric data needs continue to increase. Along with these additional bandwidth requirements, the new contract aims to include more stringent encryption policies to allow for secure wireless transmission, which must meet the Electronic Biometric Transmission Specification. This is a newer encryption standard that is becoming the de facto standard in biometric transmission.

Finally, this project also has political motivations that were key factors in creation. As a system that will involve high levels of sensitive data, the need for a non-publicly available system for sole use within government bodies is essential to ensure security. Additionally, there are many competing products that are being used in other countries’ government bodies. However, the companies designing these products are under contract to these external governing bodies that are not a part of NATO. As a result, this project is also motivated by the fact that there needs to be a system developed by a country in NATO. Overall, there are many key motivating factors to the incentive behind creating this product and our group believes that we can achieve most of the requirements set out by NATO and secondary stakeholders within the timeframe allotted.

# Stakeholders

## Original Project Stakeholder - NATO

The North Atlantic Treaty Organization (NATO) is a multi government military alliance that was formed in 1949. The purpose of NATO is to ensure member countries maintain democratic values using politics and military. Individual countries contribute resources to this organization, and it is an international effort.

The “Tactical Handheld Multi-Modal Biometric Data Capture Storage and Matching Device” project originated from the NATO government procurement website. NATO is currently searching for a supplier from any NATO nation that can create a device with complementary objectives such as:

1. Operational in tactical/military like operations
2. Ruggedized and Waterproof
3. Operated through an App on an Android device
4. Multi-modal biometric sensing, capture, matching and storage (on board and cloud)
5. Compatibility with Northrop Grumman BioSled II devices

With the current timeline, it is unlikely to meet all objectives that NATO requires for their project, particularly objectives such as making the device tactical, ruggedized, and waterproof. For the following reasons, other primary stakeholders were researched so that there is a better match with what is delivered and the needs of the primary stakeholders. However, the current solution can be extended such that it meets the requirements given by NATO in the future.

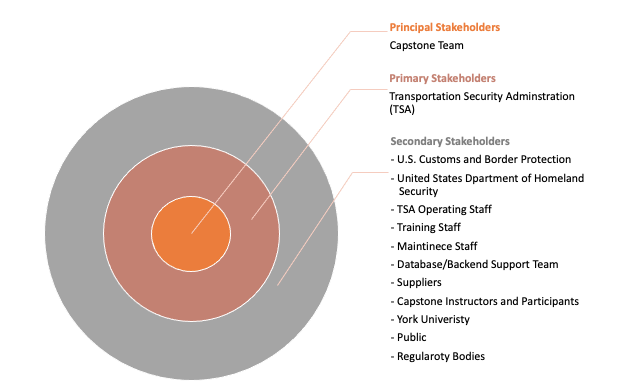
## New Project Stakeholder - TSA

The Transportation Security Administration (TSA) is part of homeland security within the United States of America. They are responsible for security and safety of travel within the USA. In September 2018, TSA released a document called the “TSA Biometrics Roadmap,” which details a plan to integrate biometric matching technology into commercial aviation travel within the United States. The main goal that TSA is trying to achieve is to automate paper-based identification processes like checking passports and IDs. Within the roadmap, TSA defined 4 goals and objectives to be achieved:

1. “Partner with CBP on Biometrics for International Travelers”
   * 1. TSA will use facial recognition at certain checkout points to identify travelers
2. “Operationalize Biometrics for TSA and Pre-Travellers”
3. Introduce multimodal biometric enrollment such as iris, fingerprint, facial scan, etc.
4. Integrate new datasets with already existing enrolled travellers in the pre travellers’ program
5. “Expand Biometrics to Additional Domestic Travelers”
6. Expand the scope enrollment and matching to travelers beyond the pre-travelers’ program
7. “Develop Supporting Infrastructure for Biometric Solutions”
8. Create infrastructure that can be utilized by other parties such as the Department of Homeland Security (DHS), and other federal agencies.
9. Create standard, policies, development, and capture roadmaps the detail the use of the system

Based on this roadmap, the objectives are very similar to the project provided by NATO. TSA is also looking for a solution that does biometric matching, storage, and collection. Removing objectives like being tactile, waterproof, etc., the device being created is an appropriate solution for TSA. Due to this reason, TSA is the primary stakeholder of this project as deliverables match the needs of TSA better than NATO.

## Identifying Stakeholders



### Capstone Team

The capstone team is responsible for the engineering and development of the device. Hence, it is the primary decision maker which is consistently involved in the development of the project.

### TSA

The targeted customer is TSA who will be participating in the economic transaction with the team, making it a key stakeholder of the project. The design and performance of the product will be heavily driven by the needs and requirements of TSA.

### U.S Customs and Border Protection

This is another agency within the United States that is working on using biometric matching for a task job. Currently, Customs and Border Protection is working on a project called “Biometric Air Exit” which involves using biometric capture data to verify that non-citizens left the country. Stage 1 of the TSA roadmap involves working with this agency to fulfill their requirements and show coordination between agencies. Additionally, the two stakeholders will work together to analyze results and make improvements for future parts of the roadmap.

### United States Department of Homeland Security (DHS)

TSA plans to integrate capabilities and feedback from DHS into its plan to implement a biometrics security system. TSA must adhere to the DHS security requirements and guidelines.

### Training Staff, TSA Operating Staff & Maintenance Staff

The training, operating, and maintenance staff will be the direct users of the device. Their feedback is vital, and it is essential for the success of our project that these groups have a seamless user experience without the encounter of any operational failures or presence of bugs.

### Database/Backend Support Team

The database/backend support team is responsible for maintaining the backend system and the database to prevent data corruption, loss, or any potential threats. Their feedback is key to the successful function of the biometric system as a whole and the maintenance of security.

### Suppliers

Our team will depend on various suppliers for the provision of key components for the device such as a fingerprint sensor and therefore, regarding the suppliers as one of the stakeholders. Our potential suppliers are Spark Fun Electronics, Adafruit and Amazon.

### Capstone Instructors and Participants

These parties carry interest whenever details of the development processes are shared and whenever they participate in providing feedback and criticism to further improve the product.

### York University

York university is the institution that provides the resources and financial means for the engineering and development of this device.

### Public

The travelers who agree to provide information that is required for the biometric identification system.

### Government/Regulatory Bodies

These parties work in the interest of the public to implement regulations and guidelines that ensure the safety and privacy of the public. They help guide the development of the project so that it is ethical and adheres to regulatory guidelines.

## Other Potential Stakeholders in the Future

### NATO

This project can be extended to meet the needs of NATO in the future as mentioned before. Due to timeline constraints, meeting objectives like making it tactile will be unlikely. In the future, the biometric device can be extended to include those objectives as the overall capture and classification system will remain the same.

### Governments

There are a variety of situations where a government may want to use this device. For example, due to COVID-19, a lot of elections may be delayed as people need to leave their houses, go to a voting station, verify their identity, and cast a vote. A biometric device like this can help in this situation as the device can be used to identify a person and cast their vote. In the future, the device can be extended to cast votes.

### Police Departments

Police departments may also get to use this type of device as it can help with identification of people under arrest.

### Conferences/Events

This device can be used by event planners for places like concerts or conferences. People who are signed up or are invited to an event, can be identified biometrically upon entry.

### Hospitals

Nurses and first responders can use this device to verify the identity of people they are treating if the unconscious person does not have their identity on them. This can help in a variety of ways such as pulling up a profile of their medical history. The device can be extended to hold patients' medical history. If a first responder is using it, the device must be durable as well.

# Our Team

## Personal Project Motivators

**Joshua Abraham:** I wanted to work on a project that mixed hardware and software development. As someone who has mainly worked on the software side, I wanted to work on mobile data communications. Additionally, biometric matching is an interesting area of research and will build on my Machine Learning and Computer Vision classes.

**Zeenia Akram:** Courses I have taken in my university career have helped me gain an interest in hardware design, however this project gives me an opportunity to apply the skills in a real-world scenario. Working on this project gives me a chance to combine both my software and hardware knowledge and utilize that to contribute to this project. Also, I believe a successful prototype of this project can be useful in a variety of applications and will provide value to its stakeholders.

**Dennis Bragilevsky:** Due to the nature of our group, I wanted to work on a project that had a split between the hardware and the software. My interest in firmware allows for the integration of the two with this project. As well, my previous knowledge of CV could be applied to the facial recognition and fingerprints used in this project.

**Hossam El-Shebiny:** This project was one of the more compelling choices for me due to the challenges it presents. The time and resource constraints make this interesting for our team since we will have to face difficult decisions to design a viable product within the scope of this capstone course. This project also provides a healthy mix of hardware and software challenges especially when trying to integrate everything together into one device. I chose this project because of its apparent complexity and the challenges attached to it.

**Sam Guraya:** When entering university my major was electrical engineering. But, when I realized that I liked to code more than doing hardware and electrical design, I switched majors to computer engineering. However, for capstone I wanted to work on a project that involved both hardware and software components. My group members also had a similar mindset as we were trying to decide which project to choose.

**Brandon Loy:** I enjoy working with sensors and embedded systems. Electronics is the reason I chose electrical engineering as my degree. Throughout my courses and co-op, I gained an interest in software as well. This project is in the realm of embedded systems and offers both hardware and software challenges.

**Dalan Shakaj:** I really enjoy practical applications of knowledge that was acquired from classes taken in my university career. This project seems to fall into a great balance of hardware and software implementation and allows me to apply knowledge gained from courses such as embedded systems.

**Daniel Tarasio:** During my time as an electrical engineer I have enjoyed both hardware and software applications, and this project has both. Working in web development and design right now, it has also made me very interested in the development and design aspect of creating an android application.

## Team Skills

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MEMBER | ROLE | SOFTWARE SKILLS | HARDWARE SKILLS | INTERESTS |
| Joshua Abraham | Software Team | **Languages:**  Python, Java, MATLAB, JavaScript, Verilog  **Skills:**  Agile Dev, OOP, UX/UI Design, Computer Vision, Testing, ML, Version Control | Embedded Systems  Communication Protocols | Full-stack development  Cloud  Infrastructure  Computer Visio |
| Zeenia Akram | Hardware Team | **Languages:**  MATLAB, Python, C++, R, Fortran  **Skills:**  CAD Modelling, Thermal Analysis, Structural Analysis, FEM | Digital Circuits Antenna Design/RF Systems  Basic understanding of Embedded Systems | Data and Spectral Analysis, Algorithmic and Computational Methods |
| Dennis Bragilevsky | Software Team | **Languages:**  Python, MATLAB, Java, Verilog  **Skills:**  Agile Development, OOP, Computer Vision, Software Testing, Software Development Lifecycle, Quality Assurance | Basic understanding of embedded systems | Backend development  Firmware |
| Hossam EL-Shebiny | Hardware Team | **Languages:**  Python, MATLAB, Java, HTML & CSS, Latex,  **Skills:**  System design & Integration, Structural and Thermal design, Object oriented programming, Scientific Computation | Verilog, STK Level 2 - Master Integration Certification, NX, Solidworks, Abaqus CAE, NI Labview | Consulting Project Management System design & integration Structural and thermal design Logistics Procurement & acquisition |
| Sam Guraya | Software  Team | **Languages:** Java, Python, MATLAB, C#.  **Skills:** AWS, Computer Vision, Machine Learning, OOP, Software Development Lifecycle | Basic understanding of embedded systems | Backend development  Machine learning  Cloud infrastructure |
| Brandon Loy | Software and Hardware Team | **Languages:** Python, C  **Skills:** Electrical design, Troubleshooting,  Embedded systems | Sensors, Instrumentation, Automation, Embedded Systems | Automation, instrumentation & control, electronics |
| Dalan Shakaj | Hardware Team | **Languages:** MATLAB, Verilog, Java, C  **Skills:** 3D Modeling, Embedded Systems | 3D modelling, Basic schematic design | Embedded systems design |
| Daniel Tarasio | Software and Hardware Team | **Languages:** Java, MATLAB,  **Skills:** Beginners understanding of UI design in Swift with XCode  UX/UI design | Basic schematic design | Embedded systems design |

## Gaps in Team Skills & Solutions

**What gaps are there in the team and where do you plan to go to fill them? What aspects of the team do you know will require help/support? What voices is your team missing?**

Making an all-in-one device would require us to design a PCB capable of running smartphone hardware. The design of these PCB’s requires a team of experienced engineers as they must control RF antennas, as well as noisy processors. Furthermore, the cost of manufacturing a complex PCB in low quantities outside of our budget. The MIL-STD-810 standard requires equipment to perform in severe conditions. Some examples are gunfire shock, acidic atmosphere, and other extreme tests. Our team lacks access to this kind of test facility, making it impossible for us to test.These requirements are not possible for us to achieve in our project scope.

Unfortunately, none of the members of our group have experience with Android development. Since our product will be interfacing with an Android device, and therefore will result in communication with an Android app, the software team of our group will need to learn Android app development for the final product. Our app requires communication with external devices and reading in bytes over a serial interface. These bytes will have to be reconfigured into the fingerprint image. Transmission of the data must be compliant with the FBI’s Electronic Biometric Transmission Specification (EBTS). This will be a challenge for the team because we are missing the voice of an individual or organization who uses that system. Furthermore, we are missing the voice of the primary stakeholder, which is NATO itself. We do not have the ability to communicate with and confirm if the method that we are using to complete the requirements are up to NATO standards.

# Survey of Solutions

Currently, there are three major competing companies that have created similar products that are like the project specified by NATO. These three companies are Northrop Grumman, Ekemp, and Idemia.

Northrop Grumman has created two previous competing products and have won multiple previous government contracts for biometric devices. However, this new project proposal has many new requirements that were outside of the original goals of Northrop Grumman’s BioSled line of devices. Some major missing components are the lack of cloud-based integration, poor battery life, no data encryption, only onboard matching available. Additionally, there were many user complaints about their latest model BioSled II including data loss issues, low dependability, poor user experience, and the device was extremely costly. Finally, the system is currently not being sold, so there seems to be no new progress being made to fix these pitfalls.

Ekemp is another company that focuses on creating biometric handheld devices. These systems are targeted at similar use cases to what our system will be targeting, including law enforcement, border control, and voting verification. However, there are some pitfalls to this solution as well. The system is built as a very low-cost alternative, so as a result the parts used were extremely low quality, not meeting NATOs standards, and the software was extremely out of date. Additionally, Ekemp is owned in part by a government body not a part of NATO, which may also pose security threats, and this system is also available to the public, which could also be a security threat. Finally, this system does not currently extend to support within NATO’s current infrastructure.

The final system that could be considered a major competitor would be Idemia’s Major eGate. This system was developed for use within another NATO affiliated country and is currently being used for border control purposes in France. This system can meet all the specifications, and infrastructure requirements set by NATO as a result. However, this system is not mobile which was a major requirement of the system required by NATO. Additionally, this system is expensive and available for non-governmental bodies which could create security issues.

Overall, though there are three strong competing products that could be put towards the project proposal, no solution currently available on the market meets all the technical, physical, and political requirements set by NATO’s project proposal. Therefore, there is still value in creating an end-to-end platform that will adhere to their project requests.

# Review of Requirements

## Out of Scope Requirements

**Identify any requirements that will likely be out of scope of the specific ENG4000 project.**

While it is essential that our device capture and match data, it is not possible for us to know if we are able to interoperability merge the data with what is already captured by the Northrop Grumman BioSled II device. This is because we do not have access to their data, or any means of obtaining such access.

We cannot create this project with the ruggedized housing along with IP 65 water resistant requirements that NATO originally specified. Since this is a key requirement in the nature of the project that NATO asked for and because we cannot reach their specification, we have placed NATO as a secondary stakeholder and placed the TSA as our primary stakeholder as we believe our achievable requirements more soundly resonate with their application.

In the time frame allotted, we cannot explicitly ascertain that we can create a system that has the capabilities of 1-N matching. However, one of the core requirements we shall reach is 1-1 matching, and 1-N matching shall be an optional requirement if we have the capabilities after reaching all the predetermined requirements.

We cannot design to meet for use in tactical/military-like operational environments due to our skills and qualifications. A 3D-printed housing will be created by our group but not to the standard NATO is looking for.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID** | **Description** | **Source** | **Comment/Justification** | **Subsystem** | **Validation timing** | **Validation Approach** |
| **HW-FUNC-REG-01** | The device shall be IP65 rated for water resistance or better. | NSPA Supply Opportunity No. 20LDS067 Document | To prevent data loss from water damage and maintain device functionality. | Structural | Critical Design Phase | IP TESTING (IP65 water resistance rating) |
| **HW-FUNC-REG-02** | The device shall be ruggedized to withstand MIL-STD-810 testing or better. | NSPA Supply Opportunity No. 20LDS067 Document | To prevent data loss and functionality from physical impacts or damage. | Structural | Critical Design Phase | MIL STANDARD TESTING (MIL-STD-810 Standard) |
| **HW-FUNC-REG-03** | The fingerprint shall have a scan window greater than 2.54mmx5.08mm. | NGI-DOC-01862-1.1 (EBTS Standards Documentation) | FBI requirement | Fingerprint Sensor | Preliminary Design Phase | Check the data sheet of the sensor. |
| **SW-FUNC-25** | The device shall perform 1:N matching based on the search field of user id. | <https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf> | 1:1 matching is a core requirement from stakeholders | Backend Software | Critical Design Review | Research and implementation will be done to create a matching algorithm based off current biometric research. |
| **SW-FUNC-29** | The system shall be able to complete a 1: N matching verification process in under 30 seconds. | Software Team | Required within the TSA project outline. | Backend Software | Critical Design Review | Using lightweight and fast APIs to ensure fast responses, and the creation of multiple endpoints for matching to improve multi-user speeds. |
| **SW-FUNC-30** | The device shall be able to conduct iris scan of both eyes simultaneously. | NSPA Supply Opportunity No. 20LDS067 Document | As per request. | Iris Scanner Module | Preliminary Design Phase | TBD |
| **SW-FUNC-33** | The system shall be able to detect, classify, and store other bodily marks, scars, and tattoos | NSPA Supply Opportunity No. 20LDS067 Document | Required for NATO, but not other stakeholders. | Backend Software | Critical Design Review | Researching scar and bodily marking analysis techniques within recognition. |

## Challenging Requirements

**Identify challenging requirements that will drive the design**

The android application has many elements. It must be able to communicate with the fingerprint sensor over serial, as well as the device camera. It also must be able to transmit data in a way that is compliant with EBTS. While the team has many strong programmers, our experience in app development is limited. There are always many pitfalls associated with learning new skills. This application is the most essential part of the system and will require the most care.

## Poorly Defined Requirements

**Identify loose or poorly worded requirements that may benefit from being tightened for the purposes of the project**

The original request from NATO “*Capability of multi-modal standards-based data capture, on-board storage and matching capability by rolled and flat fingerprint scan, iris scan of both eyes simultaneously, high-resolution camera image capture of facial images and body marks, such as scars, marks, and tattoos.”* Identification and matching of individuals can be based on one, or many, biometric identifiers. The requirement should be made clearer by stating that matching can be conducted using a subset of the listed biometrics.

## Areas of Non-compliance

**Identify any areas of likely non-compliance**

The MIL-STD810 requirement requires devices to be tailored to the conditions that it will experience in its service life. Some of these requirements are very extreme, such as gunfire shock and acceleration. The means to conduct such tests on a device are out of reach to our ENG4000 group, making it impossible to test this requirement. Furthermore, implementing all the mentioned biometric sensors will be too complex given the time frame and budget constraints.

The completion of all the multi-modal scanning requirements is simply too complex to realistically implement into our preliminary design given our time constraints. Furthermore, we have shifted our primary stakeholders, such that certain forms of biometric data are no longer in the scope of the original design.

## Preliminary Verification Approach

**Propose a preliminary approach to verifying compliance with each requirement at the design phase and the final deliverable phase**

In terms of our hardware requirements, our preliminary approach shall be to identify the specifications of the proposed hardware and select our required hardware that will match the specifications decided.

As for our physical requirements, in our preliminary design phase, we shall identify the size constraints for components such as the batteries, sensors, and android device, and allocate the basic dimensions of the device to be compliant with the components chosen. In our final deliverable phase, we shall create a design that would incorporate the components chosen in such a way that they seamlessly integrate with the device.

As for our software requirements, a class diagram will be our first plan of approach in designing the software, to ensure that all the preliminary requirements are met. This class diagram will be designed with extendibility in mind in the case that we opt to reach our optional requirements as well. For the final deliverable, UML, sequence, and activity diagrams will be drawn up to explicitly illustrate the project’s behaviour.

As for our database requirements, a preliminary set of parameters linked to the user profile shall be tested to achieve functionality and basic 1-1 matching. In the final deliverable phase, the parameters will be widened to better associate with a user profile and possibly extend to our optional requirements.

As for our security requirements, preliminarily, we shall encrypt and decrypt our data accordingly. While in the final deliverable phase, identity and access management (IAM) shall be implemented based on the user of the device.

# Full Table of Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID** | **Description** | **Source** | **Comment/Justification** | **Subsystem** | **Validation timing** | **Validation Approach** |
| **HW/SW-FUNC-01** | Hardware and software shall interface in English. | NSPA Supply Opportunity No. 20LDS067 Document | As per request. | Android Device | Preliminary Design Phase | Make sure its in English. |
| **HW-FUNC-01** | The weight of the iris recognition module shall be <10 grams. | <https://www.adafruit.com/product/3100#description> | Since the device is handheld, it is important to ensure that the weight of each module is taken into consideration. The weight of the camera that will potentially be utilized for the iris recognition module is 3.4g. A PCB will also be required for the illumination control system that is estimated to be <6g. | Iris Scanner Module | Preliminary Design Phase | We will measure the weight of all the components of the iris scanner module. |
| **HW-FUNC-02** | The cost of the Iris sensor shall not exceed $55 CAD. | <https://www.adafruit.com/product/3100#description> | Cost efficiency is important as the team possesses limited funds. The cost of the camera that will potentially be utilized for the iris recognition module is $39 CAD. A PCB will also be required for the illumination control system that is estimated to cost <$15. | Iris Scanner Module | Preliminary Design Phase | The cost of each individual component can be added to obtain the cost of the iris scanner module. |
| **HW-FUNC-03** | The device storage shall be able to hold all software, including Android OS, Drivers for sensor devices and App. | NSPA Supply Opportunity No. 20LDS067 Document | Device should be able to hold all necessary software to perform its intended functionality. | Storage | Preliminary Design Phase | Check Android device storage capacity and size of all software package file sizes. |
| **HW-FUNC-04** | The device shall weigh less than 1 kilogram (< 1 kg/ 2.20462 lbs). | Ergonomics | Reduce fatigue while using the device. | Structural | Critical Design Phase | Measure the weight of each component of the device including the housing. |
| **HW-FUNC-05** | The device shall be no larger than 25cm in length x 15cm in width x 10 cm in height. | Ergonomics | To allow for easy portability and reduce fatigue. | Structural | Critical Design Phase | Measure the size of each component of the device including the housing. |
| **HW-FUNC-06** | Hardware shall be capable of running android. | NSPA Supply Opportunity No. 20LDS067 Document | As per request. | Android Device | Preliminary Design Phase | Check device compatibility with android software. |
| **HW-FUNC-07** | The iris recognition module shall be equipped with NIR LEDs. | <https://arxiv.org/pdf/2008.08220v1.pdf> | When illuminated with NIR light the iris reveals a rich structure and unique features that would not be captured in the visible light particularly in dark coloured eyes. Thus, during the acquisition of an iris image the iris shall be illuminated an NIR light. | Iris Scanner Module | Preliminary Design Phase | When designing the PCB we will confirm the LEDs are included and functional. |
| **HW-FUNC-08** | The device shall be equipped with a NIR-sensitive camera. | <https://arxiv.org/pdf/2008.08220v1.pdf> | NIR-sensitive cameras are optimized in performance in the NIR range. This is required for capturing a high-resolution image of the iris. | Iris Scanner Module | Preliminary Design Phase | Confirm the camera is NIR sensitive before purchasing it. |
| **HW-FUNC-09** | The device shall have a minimum of 32GB of onboard storage shall have expandable storage via micro SD card reader with support up to 128GB of expandability. | NSPA Supply Opportunity No. 20LDS067 Document | To allow the devices well as store a minimum of 100 unique profiles locally as well hold all necessary software packages. | Storage | Preliminary Design Phase | Check android device storage capacity and size of all software package file sizes. |
| **HW-FUNC-REG-01** | The device shall be IP65 rated for water resistance or better. | NSPA Supply Opportunity No. 20LDS067 Document | To prevent data loss from water damage and maintain device functionality. | Structural | Critical Design Phase | IP TESTING (IP65 water resistance rating) |
| **HW-FUNC-REG-02** | The device shall be ruggedized to withstand MIL-STD-810 testing or better. | NSPA Supply Opportunity No. 20LDS067 Document | To prevent data loss and functionality from physical impacts or damage. | Structural | Critical Design Phase | MIL STANDARD TESTING (MIL-STD-810 Standard) |
| **HW-FUNC-REG-03** | The fingerprint shall have a scan window greater than 2.54mmx5.08mm. | NGI-DOC-01862-1.1 (EBTS Standards Documentation) | FBI requirement | Fingerprint Sensor | Preliminary Design Phase | Check the data sheet of the sensor. |
| **HW-IF-01** | All the connected sensors shall have the same baud rate. | Hardware Team | Required for communication purposes | Hardware Interfacing | Preliminary Design Phase | All the devices chosen to be connected to the Android phone must be able to be set at the same baud rate. |
| **HW-IF-02** | The sensors shall be connected to the phone via a multiplexer that will determine which sensor shall communicate with the Android app. | Hardware Team | Required for information to not collide and allow for data traffic to operate using a bus topology | Hardware Interfacing | Preliminary Design Phase | Software selectors shall be implemented to allow for data communication through the multiplexer. |
| **HW-IF-03** | The multiplexer shall have a minimum of 4 channels to allow 4:1 operation. | Hardware Team | Required for communication purposes between the sensors and the android device | Hardware Interfacing | Preliminary Design Phase | Select a device that meets the specification. |
| **HW-IF-04** | The circuit shall communicate to the phone via the TX and RX pins of the phone. | Hardware Team | Required for communication purposes | Hardware Interfacing | Preliminary Design Phase | The TX and RX pins of the Android device will be accessed for data transmission and data receiving. |
| **HW-IF-05** | The device shall be able to be charged while connected to the sensors. | Hardware Team | Required to charge the battery without disassembling the product | Power Delivery | Preliminary Design Phase | The wiring between the device and the charging port shall be on their own breakout circuit using the 5V and ground pins located on the phone. |
| **HW-IF-06** | The fingerprint sensor shall have capability to communicate over a UART. | Standard Serial Interface | Easy to integrate with other devices | Fingerprint Sensor | Preliminary Design Phase | Check the data sheet of the sensor. |
| **HW-PERF-01** | The device shall use 2 batteries (1 extra easily replaceable battery) that will provide power at 3.7V to the android phone and the sensor device(s). | NSPA Supply Opportunity No. 20LDS067 Document | Easy swap of batteries to prolong device use time in a critical situation faced by support teams | Power Delivery | Preliminary Design Phase | Test battery voltages and battery health. |
| **HW-PERF-02** | The batteries of the device shall have a combined capacity at minimum of 4000 mAH that will allow for a minimum of 8-hour standby battery life and the extra set of replaceable batteries shall provide equivalent performance. | NSPA Supply Opportunity No. 20LDS067 Document | Providing long battery life to ensure the success of a support task(s) or a critical situation. | Power Delivery | Critical Design Phase | Battery Life Testing in CDR |
| **HW-PERF-03** | The batteries of the device shall be able to charge using 1 USB adapter with dual supply voltage (110V/220V). | NSPA Supply Opportunity No. 20LDS067 Document | Ease of use, less cables to carry for charging the device or its batteries. | Power Delivery | Preliminary Design Phase | Hardware design in PDR |
| **HW-PERF-04** | The fingerprint sensor shall have an operating current less than 50-200mA. | Fingerprint Sensors Trade Study | TBD | Fingerprint Sensor | Preliminary Design Phase | Check the data sheet of the sensor. |
| **HW-PERF-REG-01** | The fingerprint sensor shall have at least 256 levels of gray. | NGI-DOC-01862-1.1 (EBTS Standards Documentation) | This is commonly known as an 8-bit image. | Fingerprint Sensor | Preliminary Design Phase | Check the data sheet of the sensor. |
| **HW-PERF-REG-02** | The fingerprint sensor shall have a resolution greater than 500 DPI. | NGI-DOC-01862-1.1 (EBTS Standards Documentation) | Sensors with resolution around this value are readily available and fall within our budget. This resolution is sufficient to capture the details of a fingerprint such that they can be matched. | Fingerprint Sensor | Preliminary Design Phase | Check the data sheet of the sensor. |
| **SW-BKND-01** | The backend system shall store information received from device in encrypted fashion. | NSPA Supply Opportunity No. 20LDS067 Document | Required for FBI compliance for EBTS standards (NGI-DOC-01862-1.1) | Backend Software | Critical Design Phase | Data will be encrypted using encryption libraries. |
| **SW-BKND-02** | The backend system shall have the ability to control which Android biometric devices can access the app. | Software Team | There will be more than one device that will be capturing and performing biometric matching at a time. | Backend Software | After the onboard app is made. | Test if more than one onboarded android device can send and receive information to the backend system. |
| **SW-BKND-03** | The backend shall have the ability to enable/disable features on the Android app. | Software Team | Required for security purposes and lock out unknown users in case of device loss or theft. | Backend Software | Critical Design Review | Implementing flags to enable/disable features |
| **SW-FUNC-01** | The software shall be android compatible. | NSPA Supply Opportunity No. 20LDS067 Document | As per request. | Application Software | Preliminary Design Phase | Develop android app for the device and integrate with backend/online database. |
| **SW-FUNC-02** | The android app shall be capable of sending and receiving profiles from the backend database. | NSPA Supply Opportunity No. 20LDS067 Document | Required for functionality. | Android Device | Preliminary Design Phase | Send test profiles and compare to original version. |
| **SW-FUNC-03** | The database shall be implemented using a cloud relational database (Amazon RDS). | Software Team | Will help with data organization and clarity in development | Backend Software | Preliminary Design Phase | An RDS implementation shall be followed. |
| **SW-FUNC-04** | The database shall be backwards compatible with existing data stored in the HART database. | Software Team | Required for stakeholder purposes | Backend Software | Preliminary Design Phase | The same organization and parameters shall be used. |
| **SW-FUNC-05** | The profile storage system shall be able to store user information associated with a specific user (i.e. listing name, location, reason for entering, date of birth, etc.). | Software Team | Required for stakeholder purposes | Backend Software | Preliminary Design Phase | Parameters shall be added and linked to profiles. |
| **SW-FUNC-06** | The biometric information stored in database shall be accessible by users and devices with credible/correct IAM (identity and access management) roles. | Software Team | Managing access to data is  important. Roles with certain  permissions should be created  to limit and give access to devices and users | Backend Software | Accessibility can be tested during PDR  project phase | Test to see if IAM roles without correct permissions can access data. |
| **SW-FUNC-07** | The database shall be able to store images associated with a specific user (i.e. fingerprints, face scans, IR scans, etc.). | Software Team | Required for stakeholder purposes | Backend Software | Preliminary Design Phase | Images shall be added and linked to profiles within the database. |
| **SW-FUNC-08** | Amazon Web Services (AWS) shall be used to develop backend services and databases. | Software Team | Using AWS makes our backend system easily extendable, maintainable and reliable. | Backend Software | Preliminary Design Phase | Research AWS documentation, use AWS databases and servers. |
| **SW-FUNC-09** | The backend system shall use AWS Lambda to send user information to an endpoint to create the user profile. | Software Team | Lambda is a serverless service provided by AWS. It allows for simple integration and setup. Apps also need a way to tell the backend system to create a profile which will be done by calling this endpoint. | Backend Software | Preliminary Design Phase | Create lambda endpoint, using AWS console. Call lambda through API calls to see if profiles can be  created. |
| **SW-FUNC-10** | Employees creating profiles and doing biometric scanning shall get authentication access (login) through backend system to perform task. | Software Team | Required for security purposes | Backend Software | Critical Design Review | Proper login credentials shall be distributed to authorized users. |
| **SW-FUNC-11** | Once logged out of application, employees shall not be able to access features within application. | Software Team | Required for security purposes | Backend Software | Critical Design Review | Complete disabling of the Android app’s features shall be implemented upon logout. |
| **SW-FUNC-12** | The system shall have different IAM roles that limit permissions to backend services. | Software Team | Required for security purposes | Backend Software | Critical Design Review | Login credentials shall be paired with certain level restrictions for authorized users. |
| **SW-FUNC-13** | IAM roles belonging to employees operating device shall not be able to read user biometric information. | Software Team | Required for security purposes | Backend Software | Critical Design Review | Biometric data will be restricted to any employee-level user. |
| **SW-FUNC-14** | IAM roles belonging to employees operating the device shall be able to create/onboard new profiles. | Software Team | Required for security purposes | Backend Software | Critical Design Review | Onboarding users shall be  authorized to employee-level users. |
| **SW-FUNC-15** | The application shall have access to the data coming in from all sensors via the RX/TX pins on the phone. | Software Team | Required to have communication between the Hardware and Software | Application Software | Critical Design Review | A wired connection will be setup to the device, and the application will access the GPIO pin data responsible for transmission. |
| **SW-FUNC-16** | The application shall have access to the phone's camera and be able to take and store photos within the application. | Software Team | Facial recognition needs facial images, so camera data is required | Application Software | Preliminary Design Phase | Accessing the camera from an Android application. |
| **SW-FUNC-17** | The on-board application shall transmit data according to the Electronic Biometric Transmission Specification (EBTS standard). | Software Team | Required for any government level biometric transmission. | Application Software | Critical Design Review | The generated format will match the specification documentation, and examples given. |
| **SW-FUNC-18** | The on-board system will be able to encrypt all data to meet government standard, AES encryption. | Software Team | Required for security compliance. | Application Software | Critical Design Review | Using premade encryption software that meet the standards of the regulatory body and all stakeholders. |
| **SW-FUNC-19** | The on-board application will be able to connect to the UI and interact with user input. | Software Team | Required for base functionality | Application Software | Critical Design Review | By creating endpoints between the back end and front-end of the software. |
| **SW-FUNC-20** | The application shall be able to send a profile to the database for authentication, and verification. | Software Team | Required to meet the need for cloud-based infrastructure. | Application Software | Critical Design Review | Setting up secure, encrypted connections from the device to the database service. |
| **SW-FUNC-21** | The application shall be able to access internal storage to save profiles as a temporary backup. | Software Team | A current pitfall of competing products, that the stakeholder wishes to have addressed. | Application Software | Preliminary Design Phase | Maintaining a log of data saves, and responses from the database. |
| **SW-FUNC-22** | The system shall have different IAM roles that limit permissions to application services. | Software Team | Required for security purposes | Application Software | Critical Design Review | Login credentials shall be paired with certain level restrictions for authorized users. |
| **SW-FUNC-23** | Biometric matching shall be done in the AWS cloud through an AWS lambda endpoint. | Software Team | Required to have code that can do matching. Biometric devices  additionally need a way to access the matching service in order to  identify people | Backend Software | Critical Design Review | A lambda endpoint will be setup through AWS console. This endpoint will contain the code to perform the matching. |
| **SW-FUNC-24** | The device shall perform 1:1 matching based on the search field of user id. | <https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf> | 1:1 matching is a core requirement from stakeholders | Backend Software | Critical Design Review | Research and implementation will be done to create a matching algorithm based off current biometric research. |
| **SW-FUNC-25** | The device shall perform 1: N matching based on the search field of user id. | <https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf> | 1:1 matching is a core requirement from stakeholders | Backend Software | Critical Design Review | Research and implementation will be done to create a matching algorithm based off current biometric research. |
| **SW-FUNC-26** | Matching shall be done using at least two different biometric data (face photo, and fingerprint). | <https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf> | Required that the system developed is multimodal, and so having at least two biometric readings is essential. | Backend Software | Critical Design Review | Multiple matching algorithms with confidence intervals will be developed, to ensure there is a high degree of confidence of a match, no match scenario. |
| **SW-FUNC-27** | The system will be able to detect whether the data transmitted is high enough quality to make a confident match. | Software Team | This is not an explicit requirement; however, this will help to make the system more secure. Security is a critical aspect of this project. | Backend Software | Critical Design Review | Using a confidence interval approach, and the EBTS approach quality of scans can be confirmed with respect to saved profiles and standards. |
| **SW-FUNC-28** | The system shall be able to complete a 1:1 matching verification process in under 30 seconds. | Software Team | Required within the TSA project outline. | Backend Software | Critical Design Review | Using lightweight and fast APIs to ensure fast responses, and the creation of multiple endpoints for matching to improve multi-user speeds. |
| **SW-FUNC-29** | The system shall be able to complete a 1: N matching verification process in under 30 seconds. | Software Team | Required within the TSA project outline. | Backend Software | Critical Design Review | Using fast APIs to ensure fast responses, and the creation of multiple endpoints for matching to improve speeds. |
| **SW-FUNC-30** | The device shall be able to conduct iris scan of both eyes simultaneously. | NSPA Supply Opportunity No. 20LDS067 Document | As per request. | Iris Scanner Module | Preliminary Design Phase | TBD |
| **SW-FUNC-31** | The software shall be capable of presentation attack detection including detecting printed images and textured contact lenses. | NSPA Supply Opportunity No. 20LDS067 Document | Given the nature of our project, security is a crucial element that cannot be compromised. Thus, it is vital that the iris recognition software is spoof resistant. | Iris Scanner Module | Testing Phase | Once the iris recognition software is ready, we will test whether the software is able to detect when a printed image or textured lens is presented. |
| **SW-FUNC-32** | The system shall send a match or no-match response to verify a hit within the database. | NSPA Supply Opportunity No. 20LDS067 Document | Matching responses are a core requirement of the project. | Backend Software | Critical Design Review | Research and implementation will be done to create a matching algorithm based off current biometric research. |
| **SW-FUNC-33** | The system shall be able to detect, classify, and store other bodily marks including scars, and tattoos | NSPA Supply Opportunity No. 20LDS067 Document | Required for NATO, but not other stakeholders. | Backend Software | Critical Design Review | Researching scar and bodily marking analysis techniques within recognition. |
| **SW-FUNC-34** | The system shall be able to perform a data erase of all sensitive data if requested by the application | NSPA Supply Opportunity No. 20LDS067 Document | An explicit security requirement | Backend Software | Critical Design Review | Test the ability to do a data erase, without leaving unsee fragments behind. |
| **SW-IF-01** | The application shall be able to access all the data from the hardware controllers when doing a data capture sequence. | SW Team | The application should be able to read in all data captured from sensors (Iris, camera, fingerprint sensors). | Application Software | Preliminary Design Phase | Check if data is read in for profile creation. |
| **SW-PERF-01** | Baud rate shall be at least 9600 bps | Hardware Team | Required for communication purposes | Hardware Interfacing | Preliminary Design Phase | Select a device that can be set to the appropriate baud rate |
| **SW-PERF-02** | Iris recognition shall be completed in <1.8 seconds. | <https://arxiv.org/pdf/2008.08220v1.pdf> | The fastest achievable running time for iris recognition using the lightweight image complexity-guided convolutional network that we plan to use for segmentation is 1.6 (+/- 0.2) seconds. A lightweight segmentation network is required so that it does not exceed the computing power and memory of Raspberry Pi. | Iris Scanner Module | Testing Phase | Once the iris recognition software is ready, we will test to check if running  time of the iris recognition is in the given range. |
| **SW-PERF-03** | The running time of presentation attack detection shall be <5 seconds. | <https://arxiv.org/pdf/2008.08220v1.pdf> | Evaluation of the presentation attack detection methods available open source show that the most accurate method has a running time of 4.5 (+/- 5) seconds. As security is priority in this project, we must choose the method that has the highest level of accuracy. | Iris Scanner Module | Testing Phase | Once the presentation attack detection software is ready, we will test to check if running time of the presentation attack detection is in the given range. |

# Works Cited

C. Burt, “Northrup Grumman progressing on new DHS biometric system,” *Biometric Update*, 09-May-2018. [Online]. Available: https://www.biometricupdate.com/201805/northrup-grumman-progressing-on-new-dhs-biometric-system. [Accessed: 01-Nov-2020].

Lars, *Evaluation of Contactless versus Contact Fingerprint Data, Phase 2*, vol. 1.1, May 2015.

E. González-Agulla, E. Otero-Muras, C. García-Mateo, and J. L. Alba-Castro, “A multiplatform Java wrapper for the BioAPI framework,” *Computer Standards &amp; Interfaces*, vol. 31, no. 1, pp. 186–191, 2009.

“Home,” *Northrop Grumman*, 23-Oct-2020. [Online]. Available: http://www.northropgrumman.com/. [Accessed: 01-Nov-2020].

Zhaoyuan and Adam, *Open Source Iris Recognition Hardware and Software with Presentation Attack Detection*, pp. 1–8.

NATO, “Supply Opportunity No. 20LDS067” *Tactical Handheld Multi-Modal Biometric Data Capture, Storage and Matching Device.* [Online]. Available: https://eportal.nspa.nato.int/eProcurement/FBO/eProcurementFBODetails.aspx?OpportunityId=20LDS067. [Accessed: 01-Nov-2020].

ADH-Tech, “Programming Guide GT-521F52,” *Optical Fingerprint Recognition Embedded Module*, vol. 1.0, pp. 1–36, Mar. 2017.

Raj, *Real-time Identification System using Mobile Hand-held Devices: Mobile Biometrics Evaluation Framework*, pp. 1–100, Apr. 2014.

“TSA Biometrics Roadmap For Aviation Security & the Passenger Experience,” Sep. 2018.

D. Zhang, F. Liu, Q. Zhao, G. Lu, and N. Luo, “Selecting a Reference High Resolution for Fingerprint Recognition Using Minutiae and Pores,” *IEEE Transactions on Instrumentation and Measurement*, vol. 60, no. 3, pp. 863–871, 2011.