COPPERNIC
MOBILITY | CONNECTED DATA | ANALYTICS

Requirements Specification

Mobility for Border Control

Date	15 June 2021
Pages	7
Author	Rob Vandervecht

TABLE OF CONTENTS

1. OVERVIEW

The purpose of this document is to review the requirements, best practices and considerations for the utilization of mobile and/or handheld devices in the context of Border Control activities. The content of this paper is directed at the use of devices used for multiple purposes (enrollment, verification, reporting, etc.). Single-purpose devices intended for a specific function (ie. Verification only) are discussed separately.

2. DESCRIPTION

In the context of Border Control, the concept of 'Mobility' is broadly applied to a number of scenarios where fixed identification and processing equipment is not feasible or practical. This can be due to reasons such as:

- The locations of the control/verification/enrolment activities are not fixed, and their locations change regularly.
- The control/verification/enrolment activities are within a defined facility (airport, seaport, land border crossing, etc.), but the equipment used will be required at multiple locations within the facility.
- The control/verification/enrolment functions are only required intermittently by personnel performing other functions (ie. Coast Guard) and devices need to be available as required.
- Implementing fixed workstations and equipment is impractical due to cost, infrastructure, or other physical limitations.

Within the context of Mobility, there are two classifications of devices[1] intended for Border Control activities – ***Mobile Devices*** and ***Portable Handheld Devices***.

2.1. Mobile Devices

Mobile devices are portable form factor devices that can be moved from one location to another location where they are to be used. They are often stored in a fixed location or vehicle and accessed and setup when required. Similar in style to consumer 'PRO' tablets or small form factor laptops, they are designed for use on one's lap or other flat surfaces. These devices can be distinguished by their typical square/flat form factor for table or desktop use and can support either modern mobile operating systems such as Android or a typical PC/laptop operating system such as Windows. They can be deployed in protective storage/carrying cases to accompany them to their work location and may also be deployed with separate accessories as necessary.

2.2. Portable Handheld Devices

Portable handheld devices are meant for in-hand use and are typically defined by their size and ergonomics. Similar in style to consumer mobile phones or smaller tablets, they are designed to be useable for longer periods 'in hand' without fatigue. They are also designed to be 'body-worn' through accessories and holsters to enable the user to perform their duties and have the device accessible when needed. Portable Handheld devices will almost exclusively implement a mobile operating system such as Android, designed specifically for mobile connectivity and optimized battery life. In the remainder of this document, Portable Handheld devices will be referred to as simply 'Handheld Devices'.

2.3. 'Mixed' Requirements

In some situations, Border Control systems may have requirements for both Mobile and Handheld devices. In those situations, it is important to consider a common device or platform approach to optimize development, deployment and maintenance costs. Considering this, the following requirements are intended to apply to Handheld Devices for Border Control, with the understanding that such devices can typically meet all mobility requirements but not vice-versa. In the event that the application solely contains requirements for Mobile-only devices, the associated requirements can be reduced where appropriate.

[1] EES Working Group on ICT Solutions for External Borders(sea/land) Report, 26/03/2019, ISBN 978-92-95217-54-6

3. KEY MOBILITY REQUIREMENTS – BORDER CONTROL

There are numerous requirements and characteristics that can apply to Handheld devices in general. The following section selects key points that should be considered regarding the use of Handheld devices specifically for Border Control activities.

3.1. Physical Characteristics

For Handheld devices in border Control, the typical use case involves the user having the device available while they perform their typical daily duties. When a scenario exists that requires biometric enrollment or verification in the field, the device is available and used in that current environment. In order to ensure strong user satisfaction and acceptance, there is a strong focus on ergonomics and one-hand use. Device weight is a critical factor to reduce user fatigue both in the usage scenario but also for carrying the device on their person. Since the devices can be used in numerous environments, they should possess typical rugged device specifications for water resistance, drop and temperature ratings. Key requirements for consideration are:

- Device optimized for continuous, one-hand use. Ergonomic design with handstrap.
- Weight less than 1Kg for reduced operator fatigue
- Holster or other accessories required for carrying device for an entire work shift without impeding activity
- Environmental ratings: IP64 or better, 4 foot-drop

3.2. Performance & Operation

For Handheld use cases there are a number of key requirements that are significantly different from Mobile Device use cases. The most obvious one is the use of a true mobile operating system such as Android, which despite its consumer origins, is now the de facto operating system for all durable/rugged enterprise handheld devices. It provides benefits in the areas of wireless communication management, battery/power optimization, and 'instant-on' device start up times. These are key requirements to ensure that the device is ready to operate at a moment's notice when required.

Due to the availability requirements, mobile use cases can drive different requirements in terms of battery life. The size of the battery is not the only determining factor in regard to operational autonomy. Significant factors that can affect operational battery life are primarily driven by the expected use scenario – number of fingerprint scans, face or Iris scans, data sent over wireless link, and computational load placed on the processor. Beyond that, the method in which the device is put into standby mode between uses will affect battery life. As mentioned earlier, Android is optimized for 'instant-on' in terms of establishing communications and running applications when coming out of a standby mode, while still providing superior battery life. It also has preferred functionality for quickly recovering from system or application errors and restarts. In some situations, for mobile-only use cases, the need for rapid start up, communication and error management are not as critical, which can lead to situations where operating systems such as Windows can be utilized. Overall, key Handheld requirements for consideration are:

- Mobile Specific Operating System (Android 9 minimum), 8-Core processor(minimum)
- User-replaceable battery with functional battery life > 10 hrs (Defined Usage Scenario – see Table 1)

Example Active Usage Profile (Estimated 10-hour shift)	
Deep Sleep Profile (>1 sec start-up) **Standby** Profile (<1 sec start-up) **Active** Profile (Display on, communication active)	0% 40% 60%
Enrollment Process – 10 Fingerprint capture, Photo/Iris, Document capture, database record / template processing, data comms	50 / shift
Validation Process 1 – ID document capture (NFC or optical), local processing, data comms	100 / shift
Validation Process 2 – Fingerprint capture, local processing, data comms	50 / shift

Table 1 – Sample Defined Usage Scenario

3.3. Communications & Security

Information and device security is critical in applications involving confidential identity information. Devices that are intended to manage this information need to have trusted supply chains and software integration processes to ensure the avoidance of untrusted code, backdoors, malware, etc. Key requirements for consideration:

- Defined / trusted supply chain for software integration and control.
- Auditable secure operating system (OS) source code
- Support for Secure Boot in combination with a secure element
- Support for Secure application development environments / application hardening tools specific to Mobile applications.

3.4. Data Capture & Biometrics

3.4.1. Fingerprint Capture

The mobility aspect of the use case for Border Control affects certain key requirements for the ability to capture fingerprints. As the usage environment is constantly changing, the fingerprint capture technology needs to be unaffected by sunlight and other external lights sources. It also needs to be durable from a drop and vibration perspective and resistant to scratches or other surface damage that may affect capture performance. Key requirements for consideration include:

- Supports FAP50, FBI Appendix F certified, Fingerprint capture technology designed and optimized for Mobile applications.
- Operates in varying conditions – bright sunlight/external lighting, dusty/dirty, varying temperature cold/hot/damp; without affecting capture performance.
- Implements non-glass platen (scratch resistance) and avoids use of internal prisms (fragility) with no necessity for replaceable light sources or membranes.

3.4.2. Face Image Capture

The Handheld device will be provisioned with an application or SDK that supports the necessary facial recognition requirements. The camera hardware that supports this should take into account the following requirements:

- Minimum 13MP autofocus camera, 3000x4000 pixels, multiple LED lighting system
- Ergonomic camera implementation for holding and aiming to reduce user fatigue.

3.5. Device Management Functions

Professional Handheld device deployments are often accompanied by Enterprise-class Mobile Device Management (MDM) solutions to manage, monitor and secure devices. While it is not always a firm requirement at project launch, any chosen devices should support MDM solutions if required in the future.

- Enterprise class Mobile Device Management functions include mandatory functions such as Device enrollment, remote assist, remote wipe, kiosk mode, etc.

4. SUMMARY

Requirements for biometric Border Control applications very depending on whether they are Mobile or Handheld use cases (or both). A checklist summary of the requirements reviewed in this document appears in Appendix 1.

ABOUT THE AUTHOR
Rob Vandervecht is an accomplished industry veteran with over 25 years experience in mobile computing, biometrics and security applications. He has defined and designed solutions for companies like Psion Teklogix, Motorola Solutions, Tyco Security Products and Thales. He is presently the Chief Marketing Officer at Coppernic.

5. APPENDIX 1 – MOBILITY REQUIREMENT CHECKLIST FOR BORDER CONTROL

Category	Requirement - Handheld Applications	Requirement Changes - Mobile-Only Applications
Physical Characteristics	Device optimized for in-hand use. Ergonomic design with handstraps.	Flat, stable design for on-table/lap usage.
Physical Characteristics	Weight < 1 kg to reduce user fatigue for continuous usage.	Weight < 2.5 Kg for intermittent usage.
Physical Characteristics	Accessory for carrying device for entire work shift without impeding regular activities.	Carrying case designed to transport device to work location.
Physical Characteristics	Environmental Ratings: IP64 or better, 4-foot drop.	
Performance & Operation	Mobile Operating System (Android 9 minimum).	Mobile (Android 9+) or Laptop (Windows 10) Operating System.
Performance & Operation	Octa(8)-core microprocessor (Min 1.8GHz).	Quad(4)-core microprocessor.
Performance & Operation	Memory: Minimum 2GB RAM + 16GB internal storage. (Optional Flash Storage)	Increased Memory & Storage required for Windows based devices.
Performance & Operation	User-replaceable battery with > 10hrs operational life. Defined usage profile with 'instant-on' (< 1 sec) functionality.	Can implement deeper sleep profiles with slower startup profile to allow for longer battery life.
Communications & Security	Documented supply chain for software integration and control.	
Communications & Security	Auditable Operation System (OS) source code.	Same requirements for Android OS. Windows based devices may not meet these requirements or rely on other typical desktop/IT processes and techniques.
Communications & Security	Secure OS boot in combination with a Secure Element.	
Communications & Security	Optional: Support for secure application development environments specific to mobile applications.	
Fingerprint Capture	Supports FAP50, FBI Appendix F certified, Fingerprint capture technology designed and optimized for Mobile applications.	
Fingerprint Capture	Operates in varying conditions – bright sunlight/external lighting, dusty/dirty, varying temperature cold/hot/damp; without affecting capture performance.	
Fingerprint Capture	Implements non-glass platen (scratch resistance) and avoids use of internal prisms (fragility) with no necessity for replaceable light sources or membranes.	
Camera	Minimum 13MP autofocus camera, 3000x4000 pixels, multiple LED lighting system.	
Camera	Ergonomic camera implementation for holding and aiming to reduce user fatigue.	
Mobile Device Management	Support for Enterprise class Mobile Device Management (MDM) functions including mandatory functions such as Device enrollment, remote assist, remote wipe, kiosk mode, etc.	Reduced Mobile Device Management functionality for Windows based devices.