SAVING LIVES
CHANGING LIVES

WFP **SCOPE**

Technical considerations for biometric registration and authentication in COVID-19 affected operations

Version V.1

This is a live document and is updated as frequently as needed.
Make sure you are referring to the latest version.

For internal use only.

WFP
World Food Programme

March 2020

Contents

The following is an overview of considerations – for more information on the topics below contact Scope Service Desk at scope.servicedesk@wfp.org and include "COVID-19" in the email or reach out to Sinan Ali sinan.ali@wfp.org.

I. Introduction

In recent years, a growing number of Country offices (COs) are collecting biometric data of beneficiaries during registration, primarily due to with weak or unavailable identity systems and/or to ensure that the assistance reaches the correct beneficiary. With the spread of COVID-19 into countries with WFP operations, WFP is trying to reduce the risk of transmission of the virus which can especially be high in case of use of contaminated items and repeated contact with contaminated surfaces. Therefore, this guidance lays out a broad framework to reduce physical contact between beneficiaries by adding measures such as alleviating the need to collect biometrics during registration exercises or use biometrics for authentication purposes. Programmatic processes where physical contact between beneficiaries can be reduced are:

I. **Registration:** The collection of biometrics can be alleviated. At beneficiary registration, ten fingerprints or/and two irises of the applicant are captured with biometric sensors. In both cases, there are overlapping contact area between successive applicants.
II. **Authentication at redemption:** If biometric or PIN authentication is used for at the time of assistance redemption, then there is brief contact between the relevant sensor: either single finger or eye area. Alternatively, if PIN authentication is set, then there is brief contact between the device PIN pad and the beneficiary's finger.

This document lays out guidance COs to consider using alternative methods to carry out registration and authentication without the use of biometrics.

II. Registration

Registration is the process of documenting (online/offline) key information of a beneficiary and his/her household in order to deliver entitlements. The current SCOPE registration process requires COs to request a configuration file from SCOPE Service Desk (SSD). There is no corporate guidance mandating the registration of beneficiaries using biometrics, however this is often a programmatic decision driven by the need to monitor duplicate beneficiaries or to enable authentication of beneficiaries at redemption. Elaborated below are steps to carry out registration without biometrics:

I. COs should request the SSD for new configurations (CONFIG) without mandatory fingerprint collection. Some COs already have this feature. As first step, the CO should review if they have a "Non-Biometric Configuration File" for registration.
II. COs should consider their caseload to ensure that the new CONFIGs can be utilized at all registration sites. The challenge is ensuring all registration sites – which are often offline – are

using updated "non-biometric" configurations files. To overcome this issue, COs will need to implement a coordination plan with SSD, area office and field offices.

III. In case of emergency and only if n.I and II. are not doable, COs could consider manually editing the configuration file using the text editor to remove mandatory field (SSD will share detailed instructions which will be shared after the CO shares the NFR)[1]

III. Authentication at Redemption

Authentication is the process of verifying whether a registered beneficiary is receiving entitlements. The current process for authentication either requires biometrics or PIN for verification, both data points are stored on the card. If biometrics data is stored on the card, the beneficiary is prompted to authenticate themselves with biometrics. In the case a PIN has also been configured, then it is used as a fallback option after 3 unsuccessful attempts with biometrics. PIN is also used as an alternative to biometrics in operations where biometrics are not collected.

Authentication process:

I. Fingerprint and/or PIN authentication can be turned off by the admin user of the mPOS device at field office level. This feature is already available. Please note that the written approval of CD, DCD or Emergency Coordinator should be provided in order to maintain an audit trail of the change.

II. Additionally, the SCOPE team and FAMOCO have released an mPOS COVID-19 Emergency version of the registration app. This offers the possibility for an admin to configure locally how authentication can be managed (e.g. fingerprints or PIN, or no authentication at all). This version of the app can be released through the Fleet Management System (FMS) to countries that require it.

IV.Additional Resources

https://download.scope.wfp.org/docs/scope_mobile/manuals/index.html

V. Step to Turn off mPOS Biometric Authentication

mPOS release 3.2 allows the admin to configure locally the way mPOS biometric authentication is managed (based on configuration already done on SCOPE). Change in such authentication mechanism needs to be authorized by the Country Director or Emergency coordinator and

communicated to the SSD (scope.servicedesk@wfp.org). Please note that the mPOS Admin role must be filled through the user form and submitted to SSD. This access will not be granted to retailers.