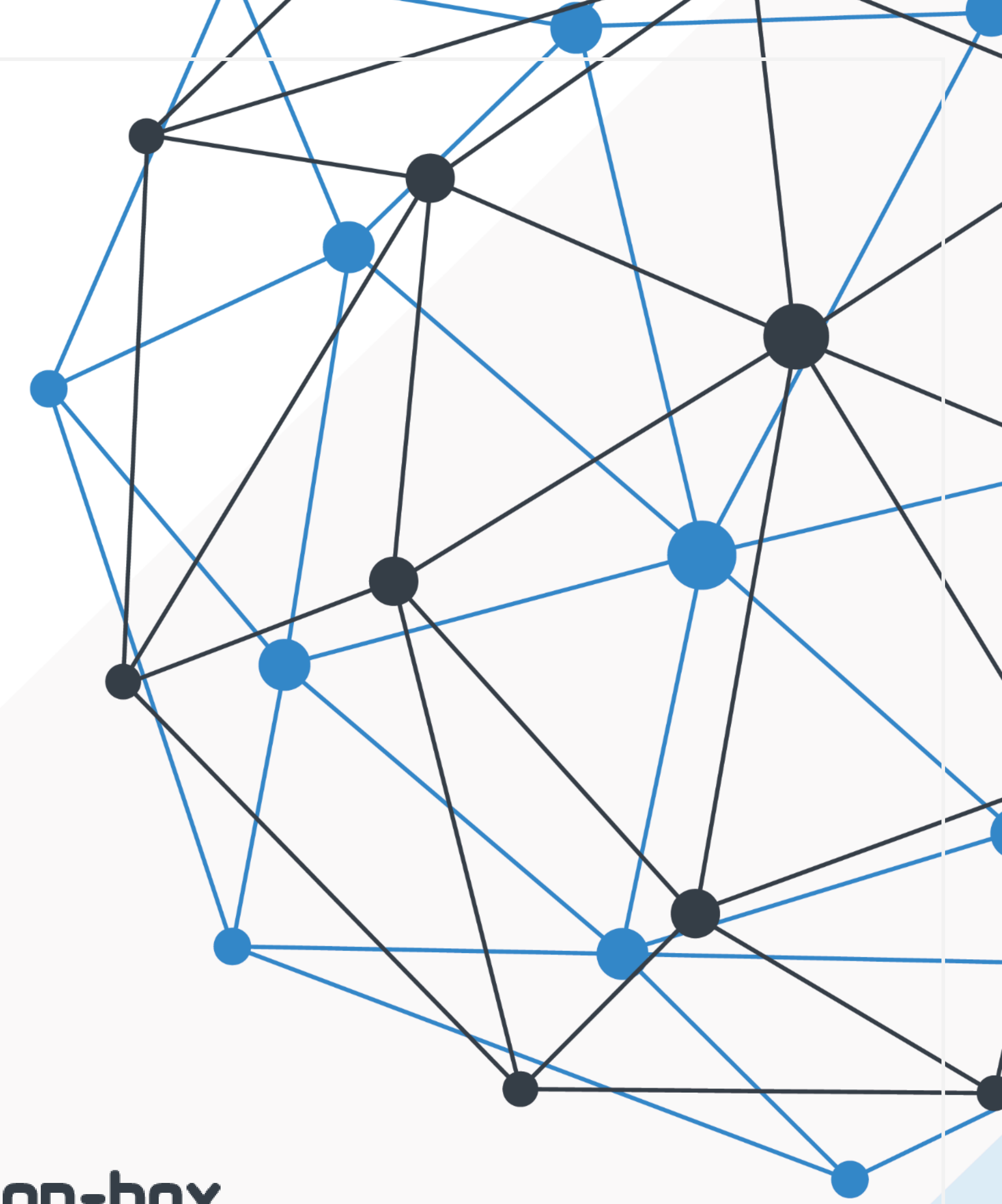


GATE-UY-SISCA-P2

Registration Desktop

COMMERCIAL IN CONFIDENCE

All rights to this document are reserved. The contents of this document are the intellectual property of Vision-Box®.
Other than user rights contractually granted, the copying, cession to third parties, or transmission of the contents of this document without its prior written consent is, consequently, forbidden. No part of this publication may be reproduced, stored, distributed, transmitted, transcribed, used, or translated into any other language, in any manner or through any means – whether graphical, electronic, or mechanical, and including its photocopying, saving and storage in any data retrieval systems – without the prior written consent of Vision-Box®.

Legal Notice
Unauthorized duplication or usage of the information presented in this document, partially or in full, and in printed format or in any other manner or through any other means, is expressly forbidden.
Except as otherwise stated herein, nothing contained in this document, or in further documents referenced herein, is to be construed as authority for varying the terms of any agreement or any individual contract generated under any agreement.

Limitation of responsibility
Although this document was reviewed and validated, it may contain typographical or technical errors.
This document is subject to a revision process from time to time, and such revisions shall be included in future issues thereof. Vision-Box®. may proceed to incorporate such modifications whenever required.
Vision-Box®. does not assume any responsibility for damages that may be directly or indirectly caused by errors, omissions or discrepancies which may arise between software applications, equipments and this document.

Licenses and Registered Trademarks
This publication contains references or information about the following products:
Vision-Box®, vision-box SENTRY®, VB-ePASS®, VB-eGate®, VB i-Match®, are registered trademarks of Vision-Box®; Microsoft and Windows are registered trademarks of Microsoft Corporation; PC is a registered trademark of International Business Corporation; Pentium is a registered trademark of Intel Corporation.
Other product and company names may be registered trademarks of other companies and are used exclusively for clarification purposes and user guidance, and without intention of infringing any such rights.

VISION-BOX CERTIFICATIONS

PARTNERS

TÜVRheinland CERTIFIED
Management System
ISO 9001:2015
www.tuv.com
ID 9108621701

TÜVRheinland CERTIFIED
Management System
ISO 14001:2015
www.tuv.com
ID 9108621701

CERTIFICAÇÃO DE SISTEMAS
ISO 27001
SGS

MSECB
PRIVACY BY DESIGN

STRATEGIC PARTNER
IATA
INTERNATIONAL AIR TRANSPORT ASSOCIATION

GATE-UY-SISCA-P2- Registration Desktop
System Specification

Version	Date	Changed by	Approved by	Change Details
0.1	10/02/2023	Ricardo Vendas	Rui Nunes	Document Creation
0.2	20/02/2023	Ricardo Vendas	Rui Nunes	Update Details
0.3	21/02/2023	Ricardo Vendas	Rui Nunes	Update Details
0.4	24/02/2023	Ricardo Vendas	Rui Nunes	Update Details
0.5	24.02.2023	Ricardo Vendas	Rui Nunes	Update Details
0.6	28.02.2023	Ricardo Vendas	Rui Nunes	Update BPMN
0.7	08.03.2023	Ricardo Vendas	Rui Nunes	Update Face Process BPMN

Content

Figure of Tables

1 Scope

The scope of this document is to describe the functional specifications of the solution.
It covers:

- Assisted Enrolment
- Touchpoints - Desktop
- Touchpoint equipped with additional interactive elements: Document Reader, Face Capture (face camera), Fingerprint Reader,

1.1. The context of work

1.1.1. Purpose

This document aims to establish a common understanding of the functional specification and System, for both technical and non-technical readers.

1.1.1.1. Solution Overview:

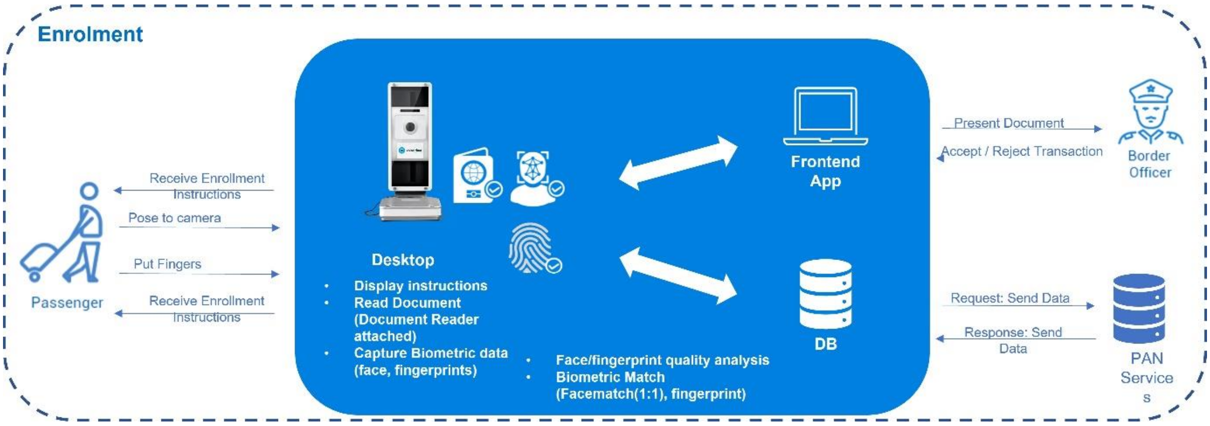

Enrolment
Receive Enrollment Instructions
Pose to camera
Put Fingers
Receive Enrollment Instructions
Passenger
Desktop
Display instructions
Read Document (Document Reader attached)
Capture Biometric data (face, fingerprints)
Face/fingerprint quality analysis
Biometric Match (Facematch(1:1), fingerprint)
Frontend App
DB
Present Document
Accept / Reject Transaction
Border Officer
Request: Send Data
Response: Send Data
PAN Service s

Figure 1: Enrolment Registration Process Solution Overview

The Enrolment Registration system will:

- Read and validate the passenger's biographic data, by scanning and capturing information from the travel document
- Capture passenger's biometric data:
  - Capturing a live photo, and verifying against the chip photo (DG2), scan photo or Immigration Service reference photo – performs a 1:1 biometric verification match
  - Capturing fingerprints and validating the quality metrics
- Confirm the authenticity of the passenger's travel document by performing visual and electronic security validations
- Send all data (Biometric and Biographic) collected during the enrolment process to the PAN Service

The PAN Service will:

- Provide an endpoint to receive captured data and transaction information
- Store the enrolment data received from the Enrolment Registration for further validation along the Border Control Process

The passenger will:

- Give the travel document to the Border Officer
- Pose for face capture (i.e., look at the Desktop face camera)
- Place the fingers on the fingerprint scanner

The Border Officer will:

- Control the progress of the transaction, instructing the passenger on how to proceed
- Place the travel document
- Ask questions to the passenger
- Jump process steps if required
- Decide on the transaction outcome

2 Enrolment

2.1. Use Case:

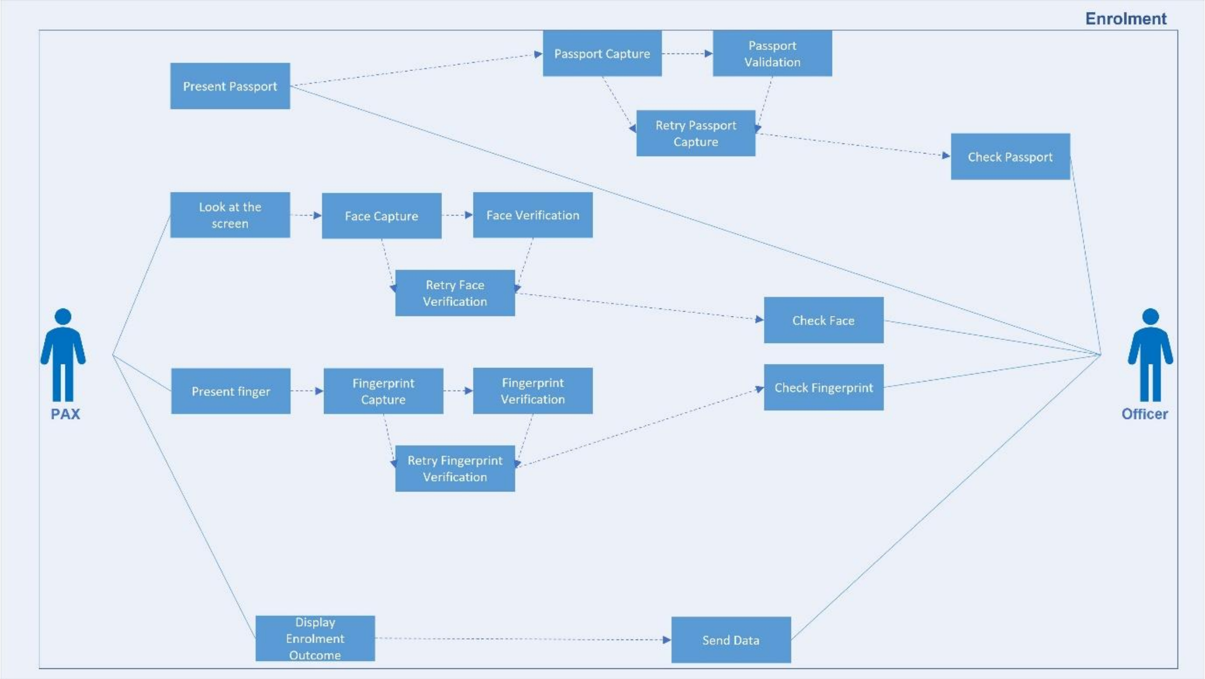


Figure 2: Use Case Enrolment

2.1.1. Preconditions

- Border Officer logged in the PAN Enrolment Application
- When ready, the Desktop shall be available for Passenger usage
- The passenger shall hold a valid travel document (non-ePassport or ePassport)

2.1.2. Actors

- Passenger: passengers intending to enter the restricted area for boarding.
- Border Officer: Border Police using the PAN Enrolment Application that controls the progress of the transaction and the Desktop.
- External System: PAN services system responsible for providing the Desktop Enrolment solution with the necessary information and responding to its requests
- Desktop Enrolment solution: a system composed of a Desktop touchpoint with the capability to capture the biographic and biometric data.

2.1.3. Assumptions

- Non-electronic and electronic Passports shall be eligible
- Vision-Box shall use the standard rules for validation ePassport/passport
- Vision-Box does not keep data from passengers that have been rejected at the Enrolment process
- Vision-Box does not store any sensitive data (biometric /biographic) in the platform
- The Desktop touchpoint is equipped with:
  - Face capture module
  - Fingerprint capture device

2.1.4. Risks

- Passenger not being cooperative to provide Biometric data

2.1.5. Transaction

<u>Initial State:</u>

- The passenger screen shall display /initial screen
- The PAN application shall display document/scan, to instruct the Border Office to place the document on the reader

<u>Transaction:</u>

- Start: when the Border Officer places the document on the reader
- End: when the Border Officer decides the transaction outcome (Accept or Reject transaction)
- Success: when all the required transaction steps are performed successfully
- Failure: when any of the required transaction steps cannot be successfully performed (e.g., biometric, or biographic data capture, biometric comparison, PAN DB External Services) or the Border Officer rejects the transaction

2.1.6. Desktop States

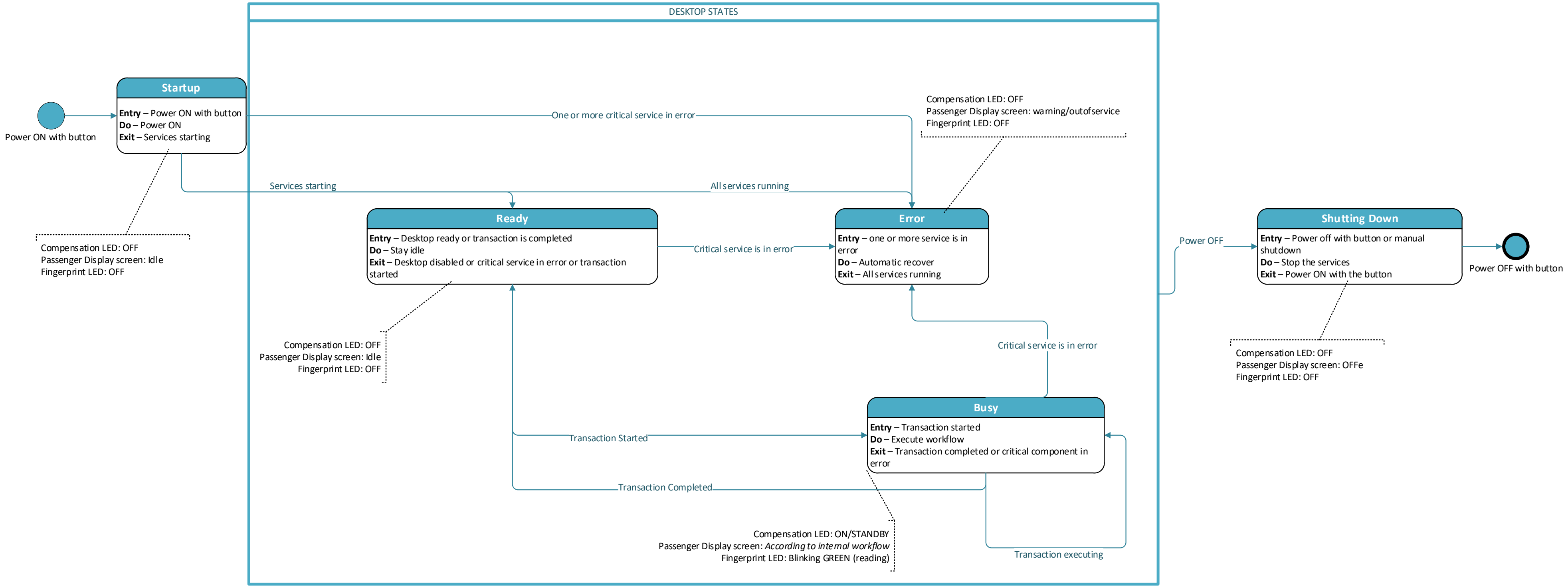

DESKTOP STATES
Power ON with button
Startup
Entry – Power ON with button
Do – Power ON
Exit – Services starting
Compensation LED: OFF
Passenger Display screen: Idle
Fingerprint LED: OFF
One or more critical service in error
Services starting
All services running
Compensation LED: OFF
Passenger Display screen: warning/outofservice
Fingerprint LED: OFF
Ready
Entry – Desktop ready or transaction is completed
Do – Stay idle
Exit – Desktop disabled or critical service in error or transaction started
Compensation LED: OFF
Passenger Display screen: Idle
Fingerprint LED: OFF
Critical service is in error
Error
Entry – one or more service is in error
Do – Automatic recover
Exit – All services running
Critical service is in error
Busy
Entry – Transaction started
Do – Execute workflow
Exit – Transaction completed or critical component in error
Transaction Started
Transaction Completed
Transaction executing
Compensation LED: ON/STANDBY
Passenger Display screen: According to internal workflow
Fingerprint LED: Blinking GREEN (reading)
Power OFF
Shutting Down
Entry – Power off with button or manual shutdown
Do – Stop the services
Exit – Power ON with the button
Power OFF with button
Compensation LED: OFF
Passenger Display screen: OFFe
Fingerprint LED: OFF

Figure 3: Desktop States

2.1.7. Overview Workflow

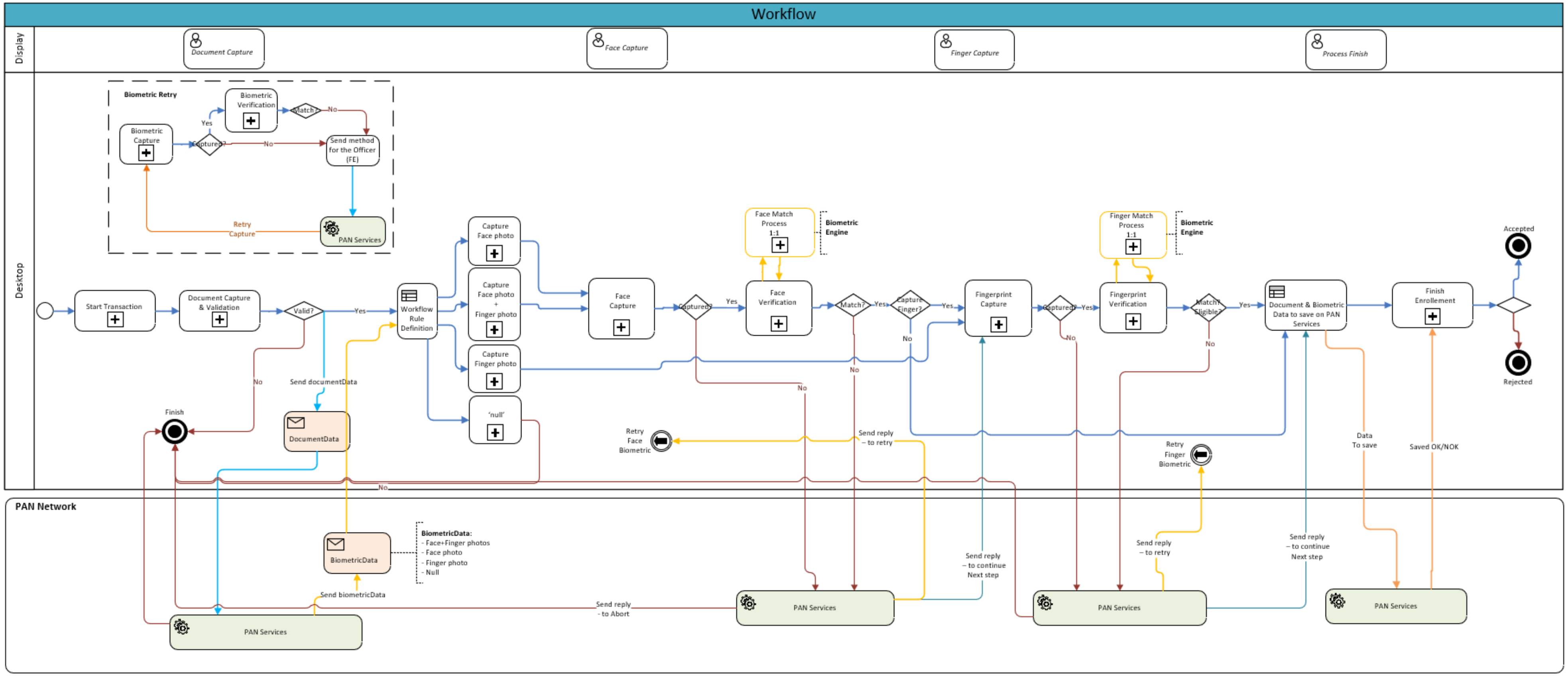


Figure 4: Overview Workflow

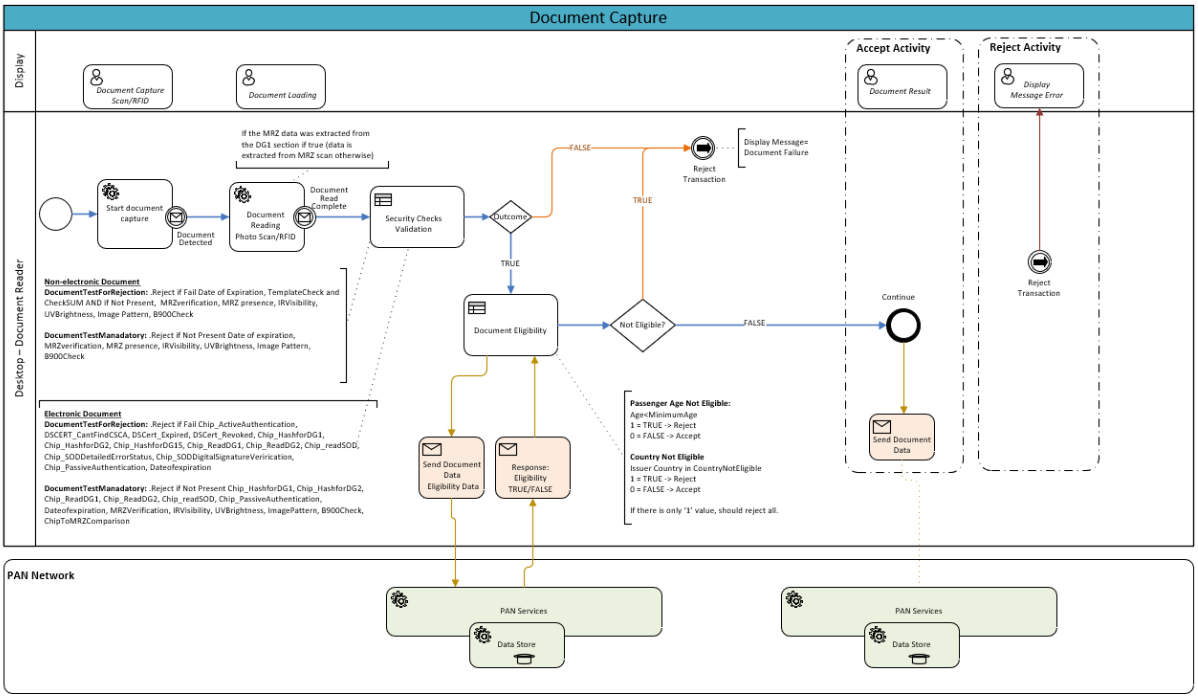
Given the Border Officer places the document on the reader, the system shall validate Document Security Checks and Passenger Eligibility, as defined in 2.1.8: Document Capture
Given the document is valid and the passenger is eligible, the transaction shall proceed to Enrolment – Check Passport, as defined in 2.1.9: Enrolment –Pan Services - Check Document.
Given the outcome of CheckDocument is FaceCollectionRequired, FingerCollectionRequired or FaceAndFingerCollectionRequired and the Border Officer decide to continue the system shall proceed to Face Verification, as defined in 2.1.10: Biometric Verification (Face)
Given the face verification succeeds and the Border Officer decides to continues the transaction:
If the outcome of CheckDocument is FaceAndFingerCollectionRequired, the flow shall proceed to Face and Finger Verification, as defined in Biometric Verification

- If the outcome of CheckDocument is FaceCollectionRequired, the flow shall proceed to as defined in 2.1.10: Biometric Verification (Face)
- If the outcome of CheckDocument is FingerCollectionRequired, the flow shall proceed to as defined in 2.1.11: Biometric Verification (Fingerprint)

2.1.17 Accept Transaction

Given any of above steps fails the system shall proceed to 2.1.15: Reject Transaction

2.1.8. Document Capture



If the MRZ data was extracted from the DG1 section if true (data is extracted from MRZ scan otherwise)

Non-electronic Document
DocumentTestForRejection: .Reject if Fail Date of Expiration, TemplateCheck and CheckSUM AND if Not Present, MRZverification, MRZ presence, IRVisibility, UVBrightness, Image Pattern, B900Check

DocumentTestManadatory: .Reject if Not Present Date of expiration, MRZverification, MRZ presence, IRVisibility, UVBrightness, Image Pattern, B900Check

Electronic Document
DocumentTestForRejection: .Reject if Fail Chip_ActiveAuthentication, DSCERT_CantFindCSCA, DSCert_Expired, DSCert_Revoked, Chip_HashforDG1, Chip_HashforDG2, Chip_HashforDG15, Chip_ReadDG1, Chip_ReadDG2, Chip_readSOD, Chip_SODDetailedErrorStatus, Chip_SODDigitalSignatureVerirication, Chip_PassiveAuthentication, Dateofexpiration

DocumentTestManadatory: .Reject if Not Present Chip_HashforDG1, Chip_HashforDG2, Chip_ReadDG1, Chip_ReadDG2, Chip_readSOD, Chip_PassiveAuthentication, Dateofexpiration, MRZVerification, IRVisibility, UVBrightness, ImagePattern, B900Check, ChipToMRZComparison

Passenger Age Not Eligible:
Age<MinimumAge
1 = TRUE -> Reject
0 = FALSE -> Accept

Country Not Eligible
Issuer Country in CountryNotEligible
1 = TRUE -> Reject
0 = FALSE -> Accept

If there is only '1' value, should reject all.

Figure 5: Document Capture subprocess

SC01. Border Officer shall place the document on the reader

Given the Border Officer presents a document on the reader, the system shall detect the document
Given a document is detected, the system shall:

- Display the screen ***document/loading***
- Display the screen ***/loading*** to inform the passenger that the process is in progress
- The system shall read document (optical scan of the document's page and document chip read, as detailed in 2.2.1.1: Document Capture – Security Check Validations

Given the document read is completed, the system shall perform Validation Rules: DocumentNotFound and evaluate the outcome

Document is Found

Given DocumentNotFound is false, the outcome is Accept Activity, and the system shall continue to Security Checks Validation

SC02. Security Checks Validation

Given validation rules succeed, the system shall perform Security Checks Validation: *DocumentTestsMandatoryAbsent* and *DocumentTestsForRejectionFail* and evaluate the outcome

SC03. Security Checks Validation Fails

Given *DocumentTestsMandatoryAbsent* is true and DocumentTestsForRejectionFail is true the outcome is Reject Transaction, and the system shall:

- Display the screen transaction/*document/failed* and send event to PAN Services that the Passport Read Failed
- Proceed to Reject Transaction, following the subprocess 2.1.15 Reject Transaction

SC04. Security Checks Validation Fail AND document tests to reject is true

Given *DocumentTestsForRejectionFail* is true, the outcome is Reject Transaction, then the system shall:

- Display the screen *transaction/document/failed* and send event to PAN Services that the Passport Read Failed
- Proceed to Reject Transaction, following the subprocess 2.1.15 Reject Transaction

SC05. Security Checks Validation OK

Given the outcome is Accept Activity, the system shall continue to Passenger Eligibility: PassengerAgeNotEligible and CountryNotEligible

SC06. Issuer Country Not Eligible

Given *CountryNotEligible* is true*,* the system shall:

- Display the screen *transaction/document/failed* and send event to PAN Services that the Passport Read Failed
- Proceed to Reject Transaction, following the subprocess 2.1.15 Reject Transaction

SC07. Age Not Eligible

Given the outcome of *PassengerAgeNotEligible* is true, the system shall:

- Display the screen *transaction/document/failed* and send event to PAN Services that the Passport Read Failed
- Proceed to Reject Transaction, following the subprocess 2.1.15 Reject Transaction

SC08. Passenger is eligible

Given the *CountryNotEligible* is false *and PassengerAgeNotEligible* is false, the system shall perform PAN Services - CheckDocument

2.1.9. Enrolment –Pan Services - Check Document

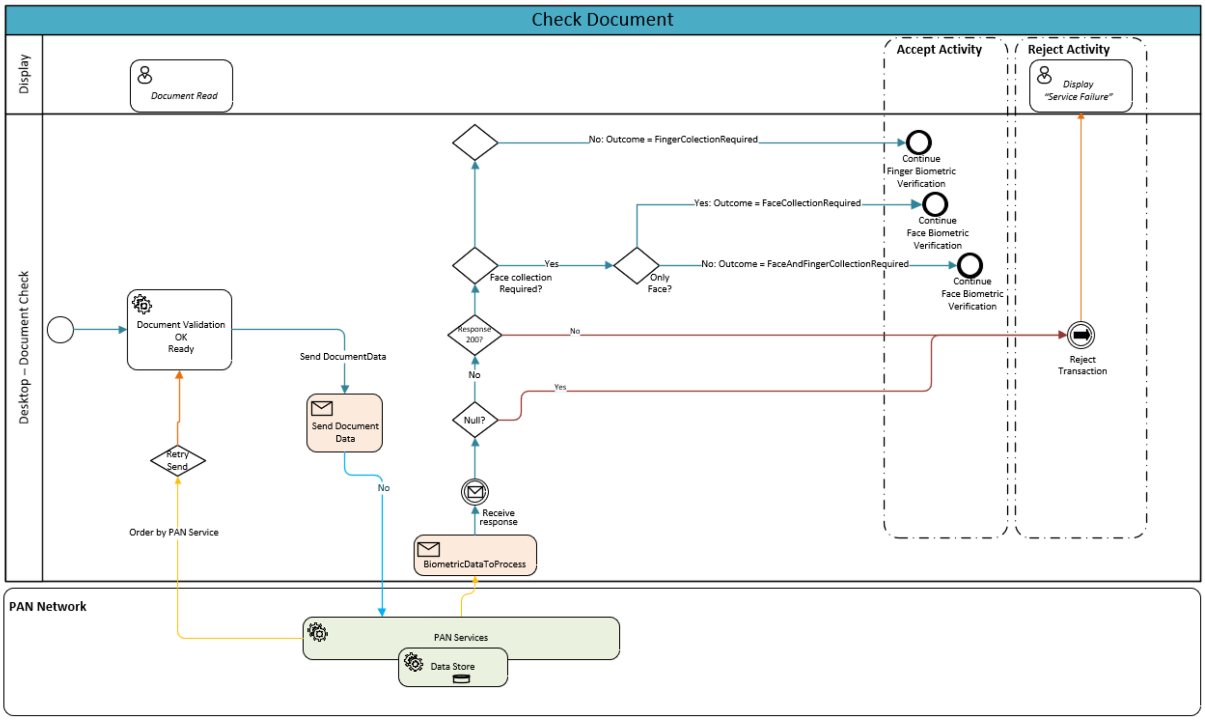

Check Document
Display
Document Read
Accept Activity
Reject Activity
Display "Service Failure"
Desktop – Document Check
Document Validation OK Ready
Send DocumentData
Send Document Data
No
Retry Send
Order by PAN Service
No: Outcome = FingerColectionRequired
Continue Finger Biometric Verification
Yes: Outcome = FaceCollectionRequired
Continue Face Biometric Verification
Yes
Face collection Required?
Only Face?
No: Outcome = FaceAndFingerCollectionRequired
Continue Face Biometric Verification
Response 200?
No
Reject Transaction
No
Yes
Null?
Receive response
BiometricDataToProcess
PAN Network
PAN Services
Data Store

Figure 6: PAN Services - CheckDocument

SC01. PAN Services – CheckDocument [DocumentData-BiometricToProcess]

Given the subprocess Document Capture is OK, then the *DocumentData* is sent to PAN Services, and PAN Services should reply with the *BiometricDataToProcess* that should be processed system shall call the PAN Services – CheckDocument

SC02. Timeout send DocumentData– CheckDocument

Given the status timeout is reached to send the DocumentData, the outcome from PAN Services is *Reject Transaction*, and the system shall:

- Display the screen transaction/failed and send event to PAN Services that the Transaction Failed
- Proceed to Reject Transaction, following the subprocess 2.1.15 Reject Transaction

SC03. Invalid response BiometricDataToProcess – CheckDocument

Given the *response* is not "200", the outcome of PAN Services – CheckDocument is *Reject Transaction*, and the system shall:

- Display the screen *transaction/failed* and send event to PAN Services that the Transaction Failed
- Proceed to Reject Transaction, following the subprocess 2.1.15 Reject Transaction

SC04. Valid response BiometricDataToProcess – CheckDocument

Given the *response* is 200 the outcome of PAN Services – CheckDocument is *Accepted Activity*, then the flow shall evaluate the content of the response.

SC05. PAN Services - Face Collection not required

Given the response to FaceCollectionRequired is false and FingerCollectionRequired is true, the outcome is FingerCollectionRequired and the system shall proceed to 2.1.11: Biometric Verification (Fingerprint)

SC06. PAN Services - Finger Collection not required

Given the response to FaceCollectionRequired is true and FingerCollectionRequired is false, the outcome is FaceCollectionRequired and the system shall proceed to 2.1.10: Biometric Verification (Face)

SC07. PAN Services - Face and Finger Collection are required

Given the response to FaceCollectionRequired is true and FingerCollectionRequired is true, the outcome is FaceAndFingerCollectionRequired and the system shall proceed to 2.1.10: Biometric Verification (Face)

SC08. PAN Services - Face and Finger Collection are not required

Given the response to FaceCollectionRequired is false and FingerCollectionRequired is false, the outcome is 'NoBiometrciCollectionRequired' and the system shall proceed to 2.1.15 Reject Transaction and the system shall:

- Display the screen *transaction/failed* and send event to PAN Services that the Transaction Failed
- Proceed to Reject Transaction, following the subprocess 2.1.15 Reject Transaction

2.1.10. Biometric Capture/Verification (Face)

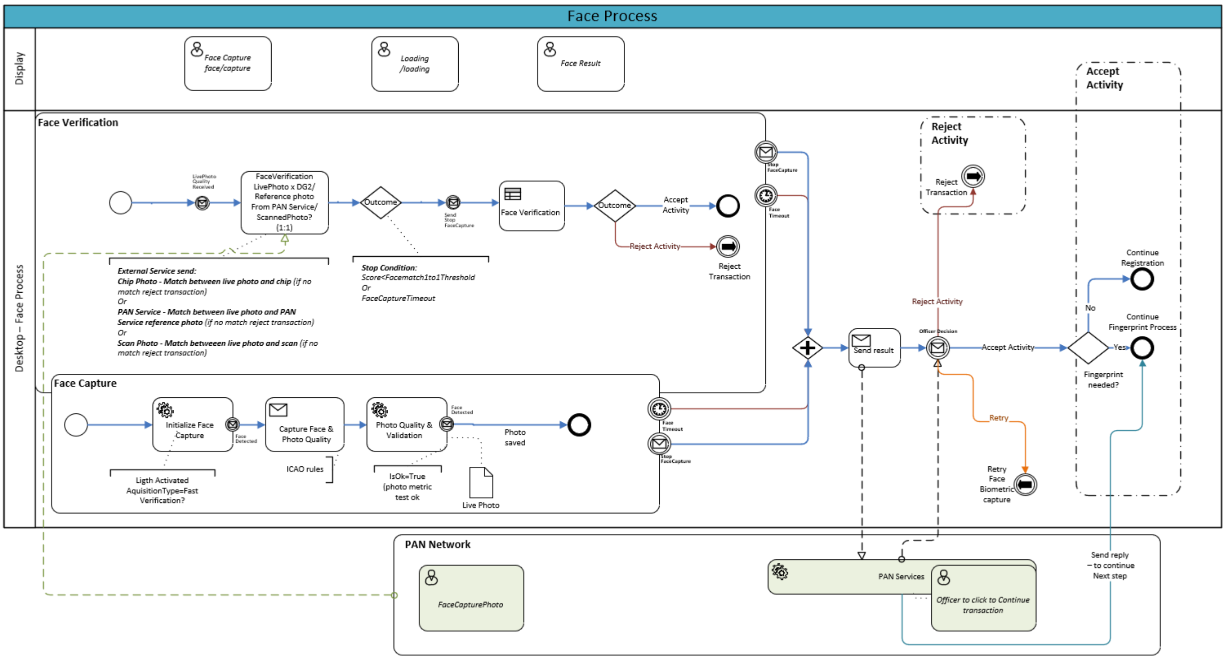


Figure 7: Biometric Verification subprocess

SC01. Timeout to detect face

Given passenger's face is not detected until the timeout, configured in *FaceTimeout*, the system shall:

- Stop the face capture
- Inform the passenger regarding the face verification failure, displaying the screen *transaction/timeout*
- Send event to PAN Service regarding the face verification failure, send event *transaction/facecapturefailed*

SC02. Timeout to capture a compliant photo

Given the timeout configured in *FaceTimeout* is reached and no compliant photos were taken, the system shall:

- Stop the face capture
- Send event to PAN Service regarding the face verification failure, send event *transaction/facecapturefailed*

SC03. Face Verification for e-Passport

Given a compliant photo is taken, the system shall perform Face Verification 1:1, by comparing the live captured face image with the e-Passport chip photo, following the configurations defined in 2.3.6: Biometric Verification.

Given the face match score is below FaceMatch1To1Threshold, the system shall:

- Send event to PAN Service regarding the face match failure, send event *transaction/matchFailed*

SC04. Face Verification for passengers with photo in PAN Service - CheckDocument

Given passenger is facematch success, the system shall perform Face Verification 1:1, by comparing the live captured face image with the image provided by the PAN Service, following the configurations defined in 2.1.10: Biometric Verification (Face)
Given the face match score is below FaceMatch1To1Threshold, the system shall:

- Send event to PAN Service regarding the face match failure, send event *transaction/matchFailed*

Given a non-electronic passport and the PAN Service does not send a photo the System should continue to Requirement SC05

SC05. Face Verification for non-e-Passport and passenger not identified by PAN Service

Given a compliant photo is taken, the system shall perform Face Verification 1:1, by comparing the live photo with the photo scanned from the passport's page, following the configurations defined in 2.3.6: Biometric Verification.
Given the face match score is below FaceMatch1To1Threshold, the system shall:

- Send event to PAN Service regarding the face match failure, send event *transaction/matchFailed*

SC06. Face match

Given the face match score is equal or above FaceMatch1To1Threshold, the system shall:

- Send event to PAN Service that the face match succeeded, send event *face/success*
- Proceed to 2.1.12 Biometric Verification (Fingers)

2.1.11. Biometric Verification (Fingerprint)

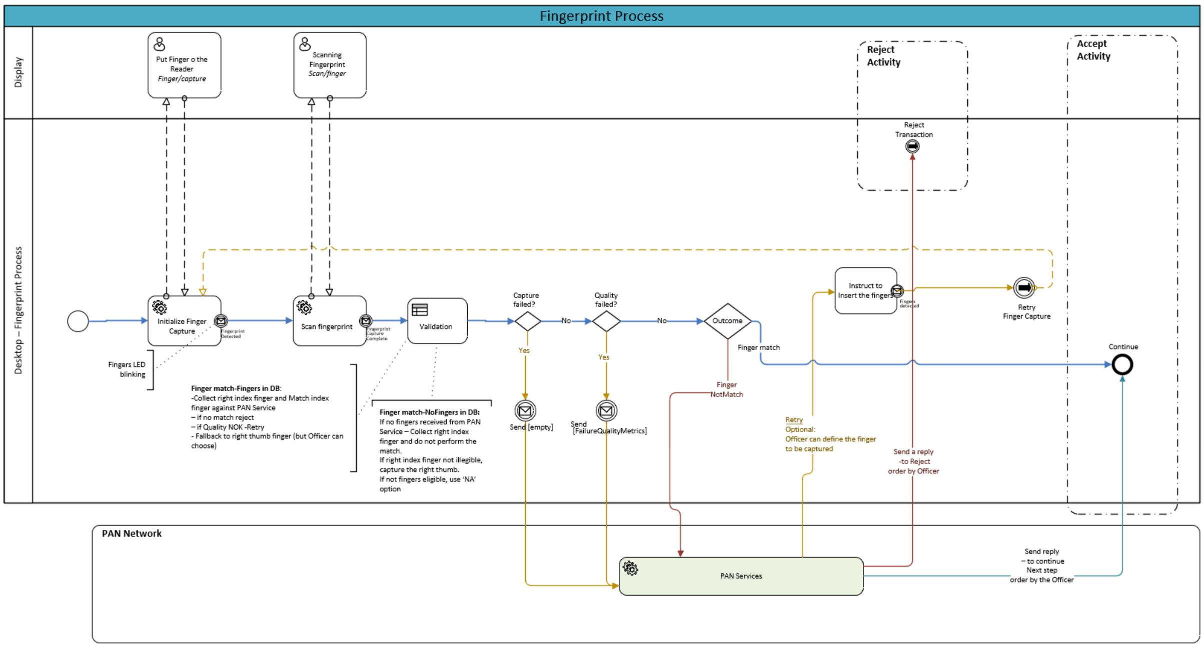

Fingerprint Process
Display
Desktop – Fingerprint Process
Put Finger o the Reader
Finger/capture
Scanning Fingerprint
Scan/finger
Initialize Finger Capture
Fingerprint Detected
Scan fingerprint
Fingerprint Capture Complete
Validation
Fingers LED blinking
Finger match-Fingers in DB:
-Collect right index finger and Match index finger against PAN Service
– if no match reject
– if Quality NOK -Retry
- Fallback to right thumb finger (but Officer can choose)
Finger match-NoFingers in DB:
If no fingers received from PAN Service – Collect right index finger and do not perform the match.
If right index finger not illegible, capture the right thumb.
If not fingers eligible, use 'NA' option
Capture failed?
Yes
No
Send [empty]
Quality failed?
Yes
No
Send [FailureQualityMetrics]
Outcome
Finger match
Finger NotMatch
Instruct to Insert the fingers
Fingers detected
Retry Finger Capture
Retry
Optional:
Officer can define the finger to be captured
Reject Activity
Reject Transaction
Send a reply -to Reject order by Officer
Accept Activity
Continue
PAN Network
PAN Services
Send reply – to continue Next step order by the Officer

Figure 8: Biometric Verification (Finger)subprocess

SC01. Passenger puts the fingers on the finger reader

Given Biometric Verification for Face succeed, the system shall:

- Instruct the passenger to place the fingers on the reader, displaying the screen *finger/capture*

Given the passenger places fingers over the finger reader, the system shall capture the fingers

SC02. Finger capture failed

Given Finger capture failed, the system shall proceed to inform PAN services with [empty value], than the following the subprocess 2.1.12 Officer Decision

SC03. Finger Capture Business Rules Validation

When finger capture is complete, the system shall:

- Perform validations according 2.1.11 Biometric Verification (Finger) validation and evaluate the outcome
- Display the screen finger/loading

SC04. Fingers Quality is Not OK

Given FingersQuality is false the system shall proceed to inform PAN services with [empty value], than the following the subprocess 2.1.12 Officer Decision

SC05. Fingers Quality OK

Given FingersQuality is true, the outcome is Accept Activity, and the system shall continue the transaction with Finger Verification 1:1

SC06. Finger Verification 1:1 if no fingerprint received from PAN Service

The system does not perform the match and continues to step SC018.

SC07. Finger Verification 1:1 if PAN Service sent fingers image

Given PAN Service Check Passport send Fingers Image, the system shall verify the match between the fingerprints received from the External System and the live fingers

SC08. Finger Verification fails.

Given the score of finger verification is below the *FingerMatchScoreThreshold1To1,* the system shall:

- Send event to PAN Service regarding the fingerprint match failure, send event transaction/matchFailed

SC09. Finger Verification succeeds

Given the score of finger verification is equal or above FingerMatch1To1Threshold, the system shall:

- Inform the passenger and the Officer that the finger verification succeeded, displaying the screen *finger/success*
- Proceed to 2.1.13 PAN Service – Send Data

2.1.12. Officer Decision

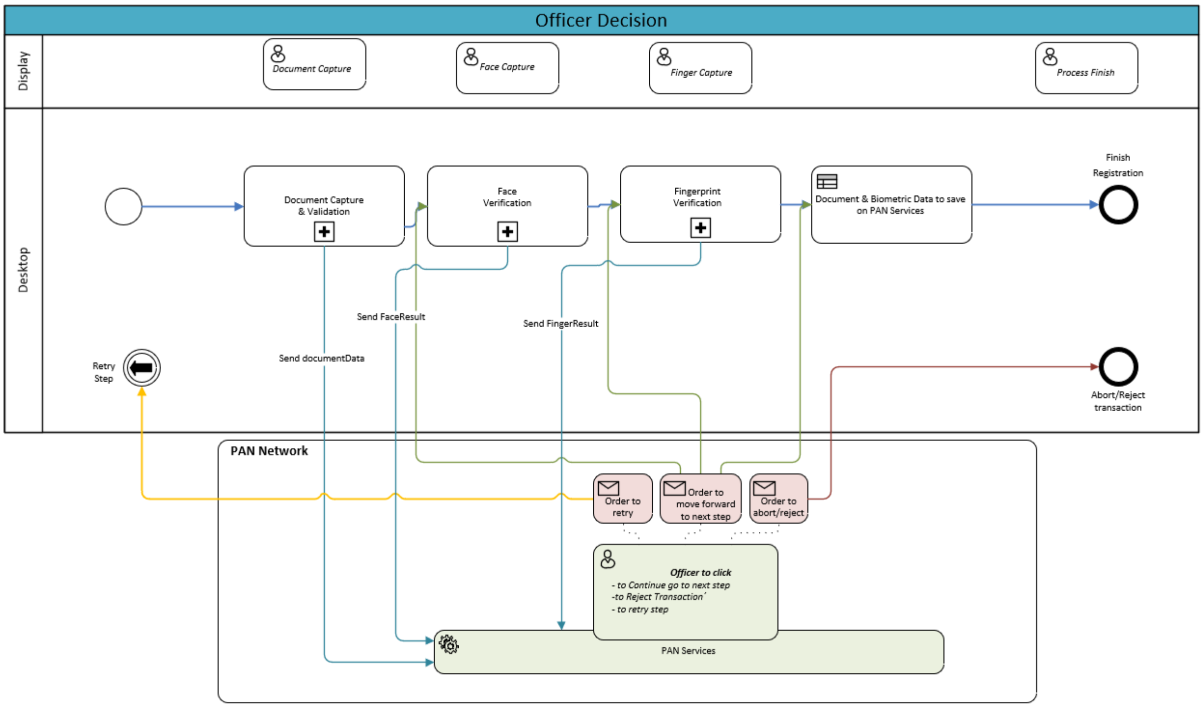


Figure 9: Officer Decision - subprocess

SC010. Document Verification Step- Officer Abort/Reject

Given the Officer Confirm the Document Data the flow step can be performed, the system shall:

- Send document verification to PAN Service/Officer application.
- Officer proceeds to 2.1.12 Officer Decision
- Proceed to 2.1.15 Reject Transaction

SC011. Face Verification Step- Officer Abort/Reject

Given the Officer Confirm the Face biometricData the flow step can be performed, the system shall:

- Send Face biometricData to PAN Service/Officer application.
- Officer proceeds to 2.1.12 Officer Decision
- Proceed to 2.1.15 Reject Transaction

SC012. Face Verification Step- Officer Order to retry step

Given the Officer Confirm the Face biometricData the flow step can be performed, the system shall:

- Send Face biometricData to PAN Service/Officer application.
- Officer proceeds to 2.1.12 Officer Decision
- Proceed to Retry Step

SC013. Face Verification Step- Officer Order to move forward to next step

Given the Officer Confirm the Face biometricData the flow step can be performed, the system shall:

- Send Face biometricData to PAN Service/Officer application.
- Officer proceeds to 2.1.12 Officer Decision
- Proceed to move to fingerProcess without face=true

SC014. Finger Verification Step- Officer Abort/Reject

Given the Officer Confirm the Finger biometricData the flow step can be performed, the system shall:

- Send Finger biometricData to PAN Service/Officer application.
- Officer proceeds to 2.1.12 Officer Decision
- Proceed to 2.1.15 Reject Transaction

SC015. Finger Verification Step- Officer Order to retry step

Given the Officer Confirm the Finger biometricData the flow step can be performed, the system shall:

- Send Finger biometricData to PAN Service/Officer application.
- Officer proceeds to 2.1.12 Officer Decision
- Proceed to Retry Step

SC016. Officer Order to retry collect fingerData

Given the Retry the capture of Finger biometricData the flow step can be performed, the system shall:

- Officer can choose the finger to capture, priority, will be the right and left hand index finger, if not, can choose another finger.
- Officer proceeds to select finger and send to Desktop to be captured.

Given the Retry the validation of Finger biometricData the flow step can be performed, the system shall:

- Officer proceeds to select ‘retry’ to send to Desktop to capture.

SC017. Finger Verification Step- Officer Order to move forward to next step

Given the Officer Confirm the Finger biometricData the flow step can be performed, the system shall:

- Send Finger biometricData to PAN Service/Officer application.
- Officer proceeds to 2.1.12 Officer Decision
- Proceed to move to registrationProcess without finger=true

2.1.13. PAN Service: Send Data

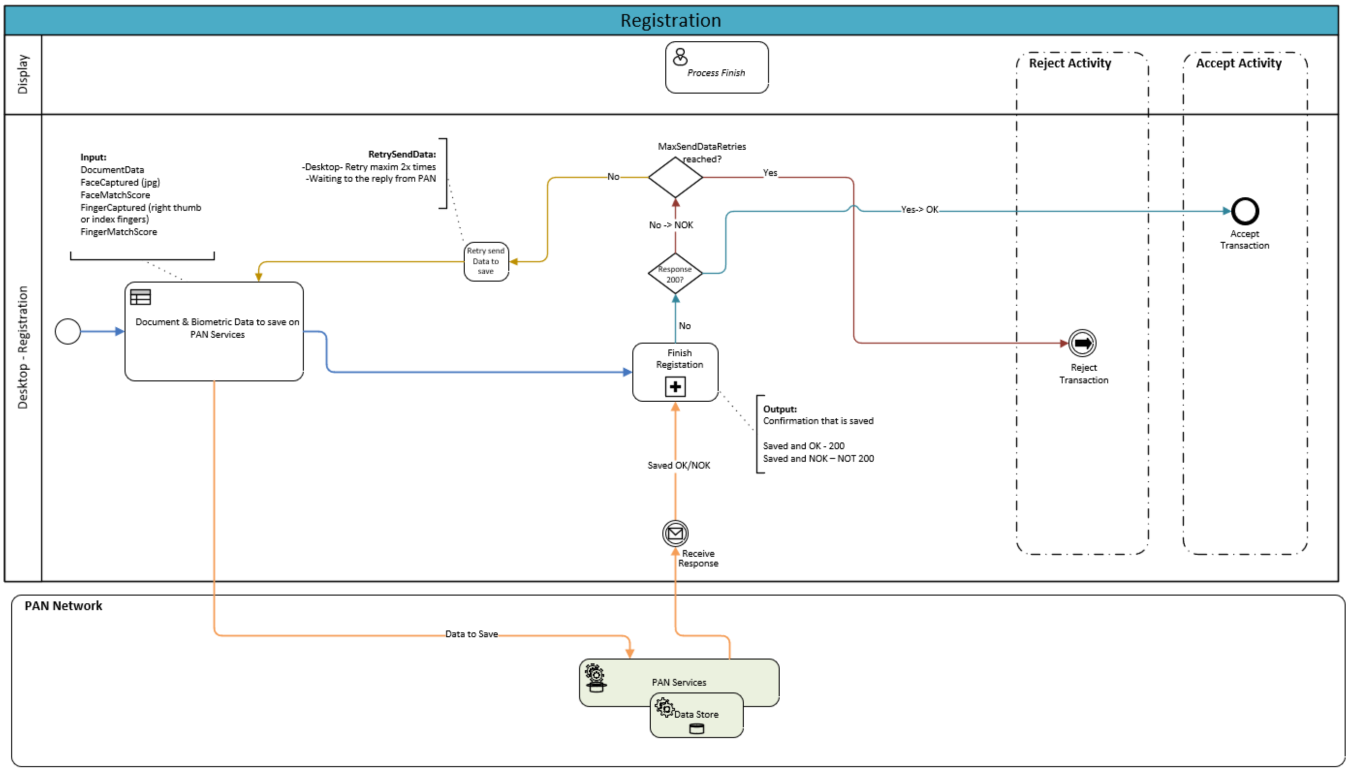


Figure 10: PAN Service – Send Data

SC018. Call PAN Service – to Send Data

Given Desktop send Document/Biometric Data to PAN Services, and wait for the reply- OK/NOK
Given the Officer Confirm the Document/Biometric Data OK the flow performs the PAN Service – Send Data – Send the reply that the Document/Biometric Data are saved on PAN Services

SC019. Error Calling PAN Service - Send Data Timeout from PAN Service

Given the status is 'timeout', the outcome of '*Document/BiometricData*' is to Retry send Data, and the system shall:

- Display the screen *transaction/timeout* to inform the border officer that the PAN Service Failed
- Proceed to Retry sending the Data to PAN Service (maxim 2x times)

SC020. Error calling PAN Service – Send Data

Given the *response* is not 200, the outcome of Send Data is *Reject Transaction*, and the system shall:

- Display the screen *transaction/failed* to inform the border officer that the External Service Failed
- Proceed to Reject Transaction, following the subprocess 2.1.15 Reject Transaction

SC021. PAN Service – Send Data

Given the *response* is 200 the outcome of Send Data is *Accept Activity*, and the system shall perform the *Registration PAN Service – Send Data*

SC022. Send Data sends NOK

Given the *response* is 200, the *result* is *NOK* and, then the system shall:

- Send to the Desktop that the Transaction ends without Success
- The system shall proceed to Reject Transaction, following the subprocess 2.1.15: Reject Transaction

2.1.14. Accept Transaction

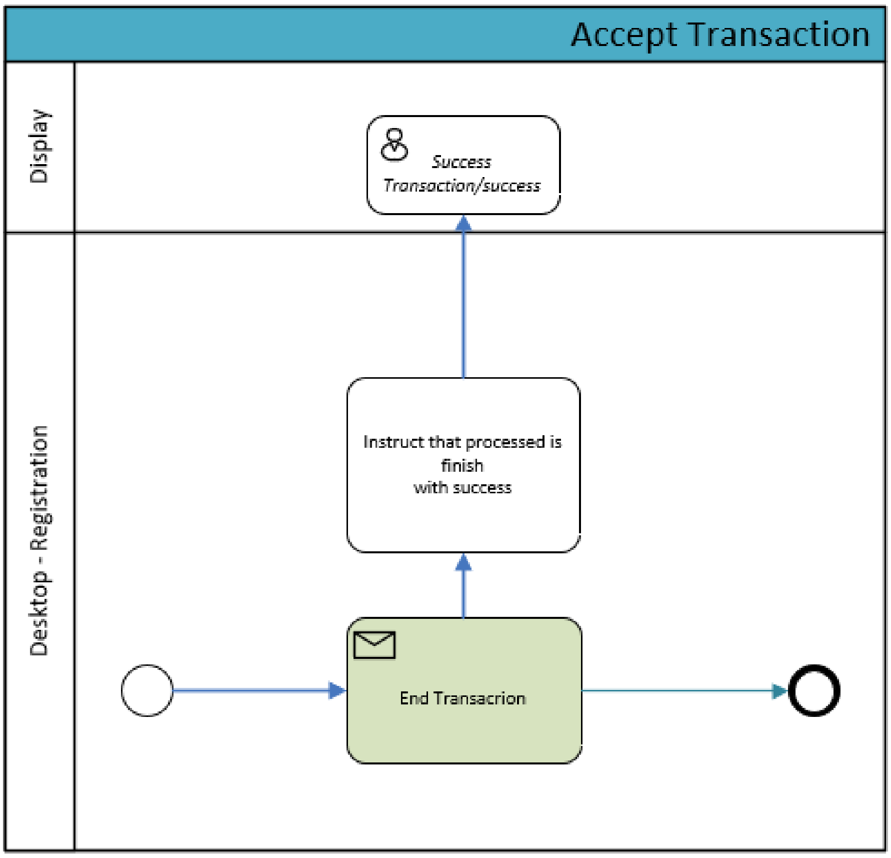


Figure 11: Accept Transaction

SC01. Instruct that the Registration went OK

Given the Officer give the Passport to the Passenger the system shall:

- Display the screen *transaction/success*, instructing passenger that the Registration went OK
- Send Data
- Return to Initial State

2.1.15. Reject Transaction

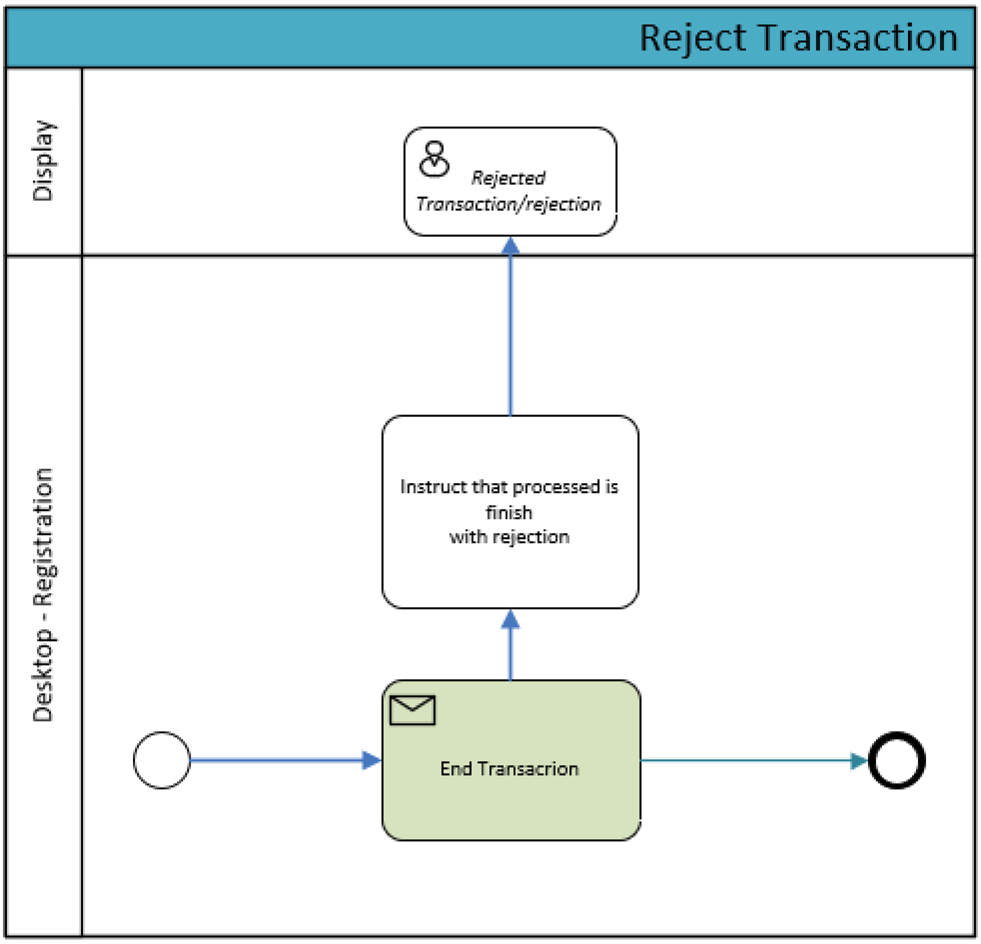

Reject Transaction
Display
Desktop - Registration
Rejected Transaction/rejection
Instruct that processed is finish with rejection
End Transacrion

Figure 12: Reject Transaction

SC01. Rejected – To Check with Officer

Given the Officer give the Passport to the Passenger the system shall:

- Display the screen *transaction/rejection*.
- Return to Initial State

2.2. Business Data

2.2.1. Rules Library

2.2.1.1. Document Capture – Security Check Validations

Name	Description	Evaluation	Outcome
Document Not Exists	Check if document exists reading MRZ data	OpticalMRZ is empty	Reject Transaction
DocumentAllRequiredSecurityChecks	Check if the Document Tests mandatory present in the Global Configuration were received	DocumentTest=Fail, in DocumentAllRequiredSecurityChecks	Reject Transaction

2.2.1.2. Document Capture - Eligibility Rules

Name	Description	Evaluation	Outcome
Country Not Eligible	Check if the document's issuer country is eligible to cross the border	Issuer Country in EligibleCountryVDesk	Reject Transaction
Passenger Age not Eligible	Check if the passenger age is eligible to perform the Enrolment	Age < MinimumAge	Reject Transaction

2.2.1.3. PAN Service – CheckDocument

Name	Description	Evaluation	Outcome
Check Passport	External Service to send passport data and receive: - Finger Print Collection Required (True or False) - Face Collection Required (True or false) - Photo image (optional); - Finger image	FaceCaptureRequired= (True, False)	Accept Activity
		FingerPrintRequired = (True or False)	Accept Activity

2.2.1.4. Biometric Verification (Face)

Name	Description	Evaluation	Outcome
Face Capture Failed	Face of the passenger was not captured	Face is not detected	Reject Transaction
Electronic Passports and non-electronic passports for non-Face Not Match*	For all ePassports check if the captured live photo matches with passport chip's photo (DG2) OR For non-electronic check if captured live photo matches with passport scan photo OR For biometric PAN Service response	FaceMatchScoreThreshold1To1< LiveThreshold FaceMatchScoreThreshold1To1< ImmigrationThreshold	Reject Transaction

	Check if live photo matches the Biometric Photo received from PAN Service		

2.2.1.5. Biometric Verification (Finger) - Finger Eligibility

Name	Description	Evaluation	Outcome
CheckDocumentWithFingers	If finger received from Biometric PAN Service	If finger received from Biometric PAN Service If no match reject	Collect right and left index finger and Match against PAN Service
CheckDocumentWithOutFingers	If no fingers received from PAN service	If no fingers received from PAN service = Collect right and left index	Collect right and left index finger and do not the match, send fingers collected to the PAN Service (CheckFingerprint) If right and index fingers not eligible, the Officer should choose which finger to capture

2.2.1.6. PAN Service – Send Data

Name	Description	Evaluation	Outcome
Send Data** *Only called in a case of a successfully transaction*	Webservice to send: - Passport data. - Live Photo - Live fingers captured - Confirmation that registrationData is saved.	Ok or NOK	External service response acknowledges. if NOK or no answer from the server Reject transaction
Send Data - Timeout	Webservice to send reply of the biometric data (face and fingers) and receive OK/NOT OK	Officer decision to reject/retry/move next step	Reject Transaction

2.3. System Configuration

2.3.1. Global Configurations - Run-time configurable

Timeout	Description	Value
DocumentCaptureTimeout	Timeout to present document	30-40 seconds
FaceTimeout	Timeout to capture and verify face	30-40 seconds
FaceMatchScoreThreshold1To1	The minimum score of the match between chip and live photos	40-50 config]
MinimumAge	The minimum age to be eligible	NOT VB
EligibleCountries	The list of countries eligible	NOT VB
FingerTimeout	Timeout to capture and verify finger	20-30 seconds
FingerQualityThreshold	Fingerprints Quality acceptance	Nist2 quality: 30-50 config
FingerMatchScoreThreshold1To1	The minimum score of the match between given fingers (External System) and live fingers	0.45

2.4. Not Run-time configurable

Timeout	Description	Value
Biometric Acquisition Type	The preset of configurations and quality metrics to capture and process capture	EnrolmentForIdentication
SrvResponsesTimeout*	Timeout to receive the response from the external service	10-40 Config

2.4.1.1. Language Mapping

Description	Language
Default Language for Border Officer interaction in the Desktop Software	Spanish

2.5. Run-time configurable

2.5.1.1. Document Validation Configurations - ePassport

Name	Description	Outcome
DocumentAllRequiredSecurityChecks	B900Check, Chip_HashforDG1, Chip_HashforDG2, Chip_ReadDG1, Chip_ReadDG2, Chip_ReadSOD, Dateofexpiration, MRZverification, ChipToMRZComparison	Reject Transaction
DocumentTestsForRejection	Chip_ActiveAuthentication, DSCert_CantFindCSCA, DSCert_Expired, DSCert_Revoked, Chip_HashforDG1, Chip_HashforDG2, Chip_HashforDG15, Chip_ReadDG1, Chip_ReadDG2 ,Chip_ReadSOD, Chip_SODDetailedErrorStatus, Chip_SODDigitalSignatureVerification, Chip_PassiveAuthentication, Dateofexpiration	Reject Transaction

2.5.1.2. Document Validation Configurations – non-ePassport

Name	Detail	Outcome
DocumentAllRequiredSecurityChecks**	B900Check, ExpirationData, Image Pattern, UV Brightness, IR visibility, Template Check, Checksum, MRZverification, MRZ presence	Reject Transaction
DocumentTestsForRejection***	ExpirationData, Template Check, Checksum	Reject Transaction

2.5.1.3. Biometric Verification (Face) configurations

Acquisition Type = EnrolmentForIdentification

Feature	Rule	Bottom Threshold	Top Threshold
Sharpness	Photo sharpness is within the values configured at calibration	1,00	
Brightness	Photo brightness is within the values configured at calibration	0,25	0,75
Hot Spots	Photo contains no hot spots	0,5	
Pose Frontalness	Face is positioned front to the camera	0,7	
Eyes Closed	Eyes closed classification	0,5	
Mouth Open	Mouth open classification	0,5	
Lighting Uniformity	Test that validates if the lighting is equally distributed on the face	0,4	
Mask Present	Validation that the face is clearly visible without any obstruction in front of it, like hair or masks	0,5	

2.5.1.4. Biometric Verification (Finger) configurations

Name	Description	Value
FingerQualityThreshold	Fingerprints Quality acceptance	Nist2 quality: 30-50 Config

2.6. List of touchpoint features

2.7. Touchpoint features not configurable

Name	Value	Description
DocumentTypes	ePassport and non-ePassport	The document type read by the document reader

2.8. Touchpoint features configurable

Name	Value	Description
AcquisitionType	EnrolmentForIdentification	The present of quality metrics and capture conditions

2.9. Instruction Screens

Desktop

ID	Description	Message (In Spanish)
Logo Screen	Idle screen with airport Logo	Airport Logo
Capturing Document	Screen informing that is capturing	
Transaction success	Screen informing Passenger that the transaction ends with success	
Transaction/rejection	Screen informing Passenger that the transaction ends with rejection	
Exit	Screen displaying the option to exit the flow	

3 Naming Conventions and Terminology

Term	Description
1:1	Biometric verification of one subject to one identity
BAC	Basic Access Control
BPMN	Business Process Management Notation
DG	Data group of the LDS
DS	Document Signature
EAC	Extended Access Control
e-Passport	Combined paper and electronic passport
IBP	Immigration and Border Protection
LDS	Logic Data Store of the RFID chip of an e-Passport
MRTD	Machine Readable Travel Documents
MRZ	Machine Readable Zone
Touchpoint	Hardware of human interaction
Workflow	The sequence of traveller processing steps forming the traveller's border check process

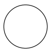
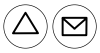
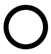
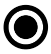
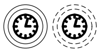
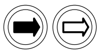
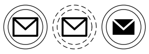
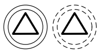
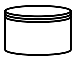
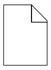
3.1. Security Checks on the Document Physical Page

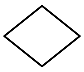
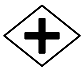
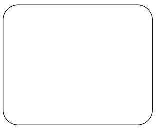
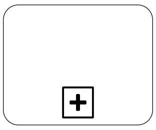
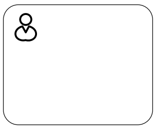
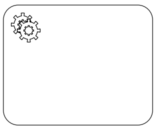
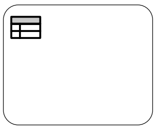
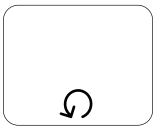
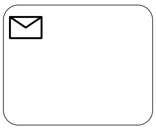
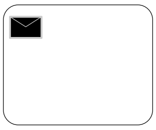
Security Check	Description
B900Check	Validation of the MRZ contrast using IR light
Date of expiration	Validation of the expiration date of the travel document
ImagePattern	Validation of the visibility of the UV patterns of the MRTD data physical page
MRZVerification	Validation of MRZ check digits
UVBrightness	Validation if the MRTD data physical page does contain dull paper
IR Visibility	Validation of the visibility of the IR elements of the MRTD data physical page
MRZPresence	Validation of MRZ presence in the passport

3.2. Security Checks on the Document Chip

Security Check	Description
Chip Hash for DG1	Validation of the hash for the chip data group #1 (MRZ data)
Chip Hash for DG2	Validation of the hash for the chip data group #2 (facial biometric image)
Chip Read DG1	Validation of the reading of the chip data group #1 (MRZ data)
Chip Read DG2	Validation of the reading of the chip data group #2 (facial biometric image). Error reading the photo stored in the chip of the MRTD.
Chip Read SOD	Validation of the reading of the Security Object
Chip to MRZ Comparison	Validation of the comparison between the information stored in the chip, the MRZ, and visual OCR (Optical Character Recognition)
Chip – Active Authentication	Validation of the chip active authentication test. The active authentication protects against MRTD cloning. This validation is available for all types of chips.
Chip – BAC / Chip - PACE	Validation of the chip using the Basic Access Control or Password Authenticated Connection Establishment
Chip – Passive Authentication	Validation of the stored information data integrity.
Chip Hash for DG14	Validation of the hash for the chip data group #14 (securing secondary biometrics (EAC))
Chip Hash for DG15	Validation of the hash for the chip data group #15 (active authentication public key)
Chip Presence	Validation that the chip is present in the MRTD. The document type was identified as an electronic MRTD but the reader cannot detect the chip.
Chip Read DG14	Validation of the reading of the chip data group #14 (securing secondary biometrics (EAC))
Chip Read DG15	Validation of the reading of the chip data group #15 (active authentication public key)
Chip SOD DigitalSignature Validation	Validation of the digital signature in the Security Object
Chip_DG14_Warnings	Non-critical warnings occurred during reading data Group 14
Chip_DG2_Warnings	Non-critical warnings occurred during reading data Group 2
Chip_HashforDG12	Validation of the hash for the chip data group #12 (additional document details)
Chip_ReadDG11	Validation of the reading of the chip data group #11 (additional person details). Error reading the photo stored in the chip of the MRTD.
Chip_ReadDG12	Validation of the reading of the chip data group #12 (additional document details). Error reading the photo stored in the chip of the MRTD.
Chip_ReadDG13	Validation of the reading of the chip data group #13 (optional details). Error reading the photo stored in the chip of the MRTD.
Chip_ReadDG3	Validation of the reading of the chip data group #3 (finger biometric image). Error reading the photo stored in the chip of the MRTD.
Chip_ReadDG7	Validation of the reading of the chip data group #7 (Displayed signature or usual mark). Error reading the photo stored in the chip of the MRTD.
Chip_SOD_Warnings	Non-critical warnings occurred during security Object validation
CSC Not Found	Validation of the presence of the Country Signer Certificate for the MRTD chip.
DSCert Expired	Validation if the Document Signer Certificate is not OK: Validation of the expiration date of the Document Signer Certificate
DSCert Revoked	Validation if the Document Signer Certificate is not OK: Validation if the Document Signer Certificate is revoked
DSCert_OK	Validation if the Document Signer Certificate is valid
LDS_DG11Present	Logical Data Structure validation - Data Group 11 presence confirmed on the chip
LDS_DG12Present	Logical Data Structure validation - Data Group 12 presence confirmed on the chip
LDS_DG13Present	Logical Data Structure validation - Data Group 13 presence confirmed on the chip
LDS_DG14Present	Logical Data Structure validation - Data Group 14 presence confirmed on the chip
LDS_DG15Present	Logical Data Structure validation - Data Group 15 presence confirmed on the chip
LDS_DG1Present	Logical Data Structure validation - Data Group 1 presence confirmed on the chip
LDS_DG2Present	Logical Data Structure validation - Data Group 2 presence confirmed on the chip
SOD Detailed Error Status	Attributes Validation of the signed chip data group attributes

5 BPMN Diagram Symbols & Notation

Symbol	Description
	Start event: Entry point of the workflow
	Catching signal start event (left): A workflow begins by catching (or handling) a signal event that was raised elsewhere Send Message event (right): A workflow begins by sending a message
	End event: Exit point of the workflow
	Terminate event: End of all workflows
	Boundary interrupting timer event (left): represents an event in any point in time which is interrup the sequence flow Boundary non-interrupting timer event (right): Represents an event in any point in time which is boundary non-interrupting.
	Throwing link event (left): represents the end point/origin of the sequence flow Catching link event (right): represents the start point/target of the sequence flow
	Interrupting message event (left): represents receiving a message. Once the message is received, the task it is attached to is immediately interrupted Non-interrupting message event (middle): represents receiving a message that will not interrupt the task it is attached to Throwing message event (right): represents sending a message, which will start a sequence flow
	Interrupting signal event (left): a signal is thrown during the execution of an activity or workflow; the workflow execution is interrupted Non-interrupting signal event (right): a signal is thrown during the execution of an activity or workflow; the workflow execution is not interrupted
	Datastore: represents a place where the process can read or write data, e.g., a database or a filing cabinet. It persists beyond the lifetime of the process instance
	Data object: any conceptual representation of data that is not necessarily a database

Symbol	Description
	Exclusive gateway: is used to model a decision in the process. When the execution arrives at this gateway, all outgoing sequence flows are evaluated in the order in which they have been defined
	Parallel gateway: the outcomes in each branch are executed simultaneously and independently
	Task: a unit of work, the job to be performed
	Subprocess: the workflow is described by a dedicated workflow diagram
	User activity: activity performed by a user, not necessarily by using an application
	Service task: is used to invoke services. Any task that uses an automated application or web service to complete the task
	Business rule task: activity performed according to a set of business rules
	Loop task: task that repeats repeatedly in sequence
	Receive task: a task that waits for the arrival of a certain message
	Send task: sends a message to another process or lane. The task is completed once the message is sent