

MB IDVERSO®
BORDER MANAGEMENT SOLUTIONS





CONTENTS

COMPANY 4-7 INTRODUCTION 8-17 SOLUTIONS 18-27 EXEMPLARY PROJECTS 28-39



COMPANY

COMPREHENSIVE SOLUTIONS

Single-Source Technology Partner

Founded in 1981 in the heart of Bavaria, the Mühlbauer Group has ever since grown to a globally acting single-source provider in the fields of PARTS & SYSTEMS, Semiconductor Related Products, Document Solution Related Products and TECURITY® Solutions. We excel in delivering state-of-the-art technology, as well as customized equipment for the end-to-end production of solutions and systems for the Smart Card, ePassport and semiconductor industry. The unique combination of the following three factors is decisive for our customer's success story:

- In-house development & research
- In-house production & assembly
- In-house training & technology transfer



Business Unit TECURITY®

Our business unit TECURITY® is established as a competent partner for the production, personalization and issuance of ePassports, ID cards, other card-related security documents, as well as fully-automatic border control systems. Furthermore, we possess the extensive know-how of the development of tailor-made security solutions. Our clients benefit from more than three decades experiential value which we have gained during the realization of over 300 ID projects worldwide.



Business Unit AUTOMATION

The business unit AUTOMATION is responsible for the development and manufacturing of all Mühlbauer technologies. We offer more than 100 different standard and customized products and intelligent software solutions for data enrollment,

border control, personalization and production management. In addition to systems for high-quality document production and personalization, we manufacture one-stop turnkey solutions for industrial image processing of cards, coins, banknotes and tubes. Moreover, we develop and produce innovative systems such as micro-chip die sorting, flexible solar cells or carrier tape equipment for specific applications in the semiconductor back-end area, as well as efficient RFID production solutions.



Business Unit PARTS & SYSTEMS

Our PARTS & SYSTEMS business segment produces high-precision components both for the manufacturing of Mühlbauer products and as a supplier to security-sensitive industries such as aerospace, motorsports, semiconductor and medical engineering.





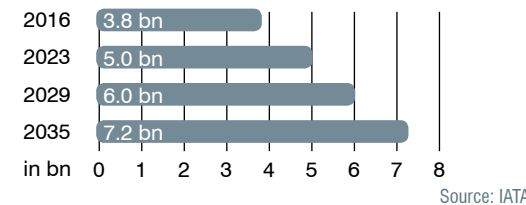
INTRODUCTION

INTRODUCTION TO BORDER MANAGEMENT

Global Challenges for Border Management

The constant globalization results in a worldwide increase of travel activities. Passenger volumes annually rise about 3.7% – a development which will result in a total of 7.2 billion flight passengers by 2035 (Source: IATA).

Development of Flight Passenger Volumes



To cope with this development, management organizations and authorities at airports, seaports and land border control points need to be provided with comprehensive solutions. Despite the higher passenger volumes, the acceleration and facilitation of border crossings has to be guaranteed, while at the same time

passenger satisfaction needs to be preserved. Due to international threats and trans-border crime, security measures also have to be enhanced. That is why future border management systems should both handle low-risk passengers in a quick, convenient and cost-effective way, and at the same time reliably identify and separate potentially high-risk travelers.

Threats & Challenges for Border Clearance

- Document fraud
- Identity fraud
- Illegal migration
- Terrorism
- Smuggling
- Human factors

State-of-the-Art Technologies

In order to efficiently handle these rising passenger numbers, the establishment of latest technologies has become essential:

- Automated Border Control (ABC) systems efficiently perform the border control process and thus expand the control capacities within a limited investment.
- Innovations like 3D face recognition allow for an even more accurate authentication of individuals.
- The use of ePassports and next generation eMRTDs does not only enhance security and facilitation during the travel document's issuance, but also during its verification process.
- Advanced Passenger Information systems are integrated into the ABC systems: they capture travelers' extended data and receive these information well in advance of their arrival.
- The Automated Border Management systems match the data with international watch lists and thus inform about stolen documents or other cases of fraud.

Advantages of Automated Border Control Systems

One of the key benefits of ABC systems is the increase of capacities for border clearance. Thus, a more efficient use of the existing – and in most cases optimized – infrastructure can be guaranteed. The investment in ABC systems allows for a faster and more efficient processing of passengers. The ABC system also allows for cost reductions, which are for example effected by the installation of self-service checks instead of desk-based checks. Further cost-intensive measures such as the expansion of the terminal infrastructure can be prevented as well. Additionally, the ABC systems implement higher verification standards for the identification of travelers – e.g. the matching with biometric information – and their travel documents.

Introducing Integrated Border Management

Mühlbauer's Integrated Border Management architecture is based on flexible software modules and thus provides tailor-made solutions based on customers' individual requirements. The design is inspired by today's border management challenges, international guidelines, such as ICAO's latest Traveler Identification Program (TRIP), and best practices. Simple check points, border posts, highly sophisticated ABC solutions, as well as local or even global border management systems for securing airports, seaports and land borders nationwide can optionally be implemented into Mühlbauer's Integrated Border Management.

Global Interoperability

Border management systems ensure facilitation and efficiency on a national basis. Worldwide security can only be enhanced by means of global interoperation between different information systems including name records, Advance Passenger Information (API) systems, visa information systems, international databases and watch lists such as Interpol databases (SLTD and Dial-Doc) and the Schengen Information Systems (SIS and SIS II). Furthermore, the border management system should be designed to process different kinds and generations of travel documents at the same time. Flexibility, also with regard to integrating future standards, is essential in order to establish global cooperation amongst authorities and agencies.



INSTRUMENTS OF BORDER MANAGEMENT

eMRTD

Electronic machine readable travel documents (eMRTDs) – ePassports, eVisa or any other electronic ID document accepted for traveling purposes – allow for the traveler’s reliable identification and verification. ICAO Doc. 9303, the international specification for eMRTDs, ensures that documents complying with these standards can be read with any suitable device or ABC unit. Thus, security and facilitation is enhanced throughout the whole process. Next to the MRZ (Machine Readable Zone) – established to simplify the capturing of the document information – lies the eMRTD which holds a storage chip containing the holder’s personal and biometric data. By employing latest PKI (Public Key Infrastructure) solutions, the documents are increasingly better protected from fraud.

With the LDS 2.0, the latest generation of ePassports is to be launched. Current ePassports are limited in their functionality, whereas

the new LDS 2.0 is an enhanced eMRTD with chip applications. These applications can both hold eVISA and advanced passenger information to secure fast access and serve as token for temporary travel records.

eVISA

As it is increasingly important to receive further information on travelers well in advance of their arrival, the visa has become an essential part of the border control process. To meet the challenges of increasing traveler volumes and to allow for facilitation for the passengers, border management solutions have to efficiently integrate the visa into the control process. Especially eVISA constitute a convenient and efficient alternative to the standardized visa application procedure.

The document contains information about the applicant, the duration and the purpose of the stay, as well as a MRZ, which – on entering the country – has to be read sepa-

ately from the verification process, leading to longer processing times. In order to render the process more efficient, the applicants can apply for an eVISA online by transmitting their personal data which are then stored in the central visa database. No certification or stamp has to be issued, the applicant only receives a soft copy via email. During the verification of the ePassport, the data is automatically matched with the visa database to check if the traveler has a valid visa. This significantly reduces processing times and enhances passenger facilitation.

Visa Information Systems

Visa information systems facilitate visa application processes and support border clearance authorities to prevent cases of fraud and – in case of the Schengen states – “visa shopping”, i.e. applying for visa to further Schengen states although a first application has already been rejected.

The visa information system contains all the information regarding visa applications, issuances, rejections, annulments and extensions by the authorities in charge. It collects the personal and biometric information of third-country applicants who intend to enter the country. During the border clearance process, the system enables authorities to smoothly verify the visa holder’s identity. By reading the traveler’s fingerprint and matching it with the data stored in the visa information system, it is ensured that the visa applicant and the visa holder are one and the same person.

Advance Passenger Information Systems

To cope with the increasing number of international challenges and threats, Advance Passenger Information Systems have been introduced. They provide information on the travelers well in advance before they enter the country. During check-in the personal data of the passengers, together with their travel document type, the country of issuance and the document number is required. The data is submitted to the authorities of the country of destination. They match the data against databases and watch lists, thus enabling the facilitation of border control and avoiding illegal entry.

Watch Lists and Databases

Watch lists are information systems with comprehensive databases, which collect relevant information. Governmental authorities have access to national and international watch lists to prevent the entry or exit of a wanted person or identify stolen documents.

Examples for Watch Lists:

- Fugitives and suspected terrorists
- Interpol Stolen and Lost Travel Document (SLTD) database which links missing travel documents to fugitives
- EdisonTD which holds genuine examples of 3000 documents from 206 countries
- Dial-Doc which shares new counterfeiters among G8 countries
- Schengen Information Systems (SIS and SIS II) which hold information on wanted and observed persons, missing persons, unwanted persons and items such as weapons



MILESTONES OF BORDER MANAGEMENT

<< MRZ >>>>
000123456 <<

1980

Standardization of MRTD

With the release of the ICAO 9303 W/MRZ standard, ICAO standardizes traveler documents. One year later, the first MRTD is introduced integrating the personal data in a format which can automatically be read out.



1995

Introduction of SIS

The Schengen States launch the Schengen Information System (SIS) for the automated distribution of information about wanted individuals. In 2013, biometrical information are added (SIS II).

2002

Introduction of automated border control units

The first ABC units are installed at airports to implement a time- and cost-efficient verification process based on biometrical information.

2004

Introduction OF eMRTD LDS 1.0

The first ePassport is issued. It includes an embedded chip containing the holder's personal data and biometrical information.

2002

Launch of Interpol Watch List and Databases

Interpol launches the Terrorism Watch List. Authorized police agencies worldwide gain instant secure access to receive information on fugitives and suspected terrorists. The Stolen and Lost Travel Documents database is introduced to avoid document misuse for terrorist activities.

2005

Initiation of BAC

The Basic Access Control (BAC) system protects the data stored on the chip. Only after reading out the MRZ and generating the key with this data, reading devices receive access.

2014

Introduction of SAC in the EU

The Supplemental Access Control (SAC) is an advanced mechanism which allows a more secure access to the data stored in the chip. By 2015, all newly issued ePassports in the EU support SAC.

2009

EAC becomes mandatory in the EU

By verifying the chip's genuineness and protecting the access to the more sensitive biometrical data stored in it, the Extended Access Control (EAC) system adds more security to the BAC.

2015

Deadline for Expiring of non-MRPs

According to ICAO standard 3.10.1, all non-machine readable passports must be out of circulation by November 2015.

2018

Possible Deprecation of BAC in the Future

BAC may become deprecated in the future. In this case, PACE will become the default access control mechanism.

2020

Going Live of Etias

In the future, travelers who do not require a visa will be screened before they arrive in the EU using the European Travel Information and Authorisation System (Etias).



INTERNATIONAL STANDARDS, PROGRAMS & GUIDELINES



CHICAGO CONVENTION ANNEX 9 FACILITATION

The Chicago Convention (1944) established the international standards for the coordination and regulation of international air travel. The standards and recommended practices (SARPs) are specified in the 19 annexes to the convention. Annex 9 focuses on all functions and procedures related to the border clearance process. This helps management organizations and authorities (e. g. contracting states implementing the standards) to optimize border control and achieve and preserve highest security standards, interoperability, as well as effective law-enforcement.



RESOLUTION 1373

The events of 9/11 did not only cause nations worldwide to focus on the importance of comprehensive border control, but also initiated the current developments in the security industry. The necessity for improved border clearance, advanced travel documents and global collaboration became apparent. The UN Security Council Resolution 1373 obliges member states to take action against international terrorism by effective border management and to enhance measures for the control of travel documents and the prevention of forgery and counterfeiting.



DOCUMENT 9303 MACHINE READABLE TRAVEL DOCUMENTS

ICAO's Doc. 9303 defines the standards and specifications eMRTDs have to comply with, e.g. the needed personal and biometric data of the holder, the MRZ and the security measures regarding data access (BAC, EAC, SAC). The major goal is to reach global interoperability of (biometric) identification and verification methods, thus ensuring efficient border crossing and worldwide security. To prevent counterfeiting and fraud, Doc. 9303 is constantly enhanced with new specifications, for example with regard to next-generation eMRTDs (LDS 2.0), which contain latest security features and technologies for secure data storage.



SCHENGEN BORDERS CODE

This code defines key rules for the management of borders to be followed by the Schengen member states. It explains how to effectively process border crossings, facilitate legitimate access to the EU and manage entry requirements and visas. Due to the abolition of checks at internal borders, unified standards are introduced at all external EU frontiers. The code also regulates the extended cooperation between member state authorities and initiated the creation of the Schengen Information Systems (SIS, SIS II) and the Visa Information System (VIS).



BEST PRACTICE GUIDELINES FOR ABC

The guidelines have established themselves as a soft standard for the design, the deployment and the operation of ABC systems. Based on a coordinated exchange of experiences, they define the benefits and basic requirements including key components such as physical barriers, document readers and biometry capture devices. The guidelines, which are meant to ensure efficient border crossing and highest security standards, focus on ABC systems used by EU citizens with ICAO Doc. 9303-compliant eMRTDs.



SMART SECURITY PROGRAM

SmartS envisions an uninterrupted passenger flow through security checkpoints at airports. Security resources are allocated and optimized. This procedure enables a real-time risk assessment without inconveniencing passengers unless potential threats are identified. The program signalsizes the development towards comprehensive solutions dealing with increasing passenger volumes. It ensures a faster, more convenient process flow for passengers, improved customer satisfaction and less delays for airlines, maximized operation efficiency and revenue for airports and advanced methods to preserve overall security for governmental authorities.





SOLUTION

SOLUTION OVERVIEW

THREE-LAYER SYSTEM

Basis for MB IDVERSO®
A three-layered software model has been created as base of the MB IDVERSO® border management solution. It classifies control and management functions in:

GLOBAL LEVEL

The central border management system administrates relevant information for border clearance and integrates external information systems into the clearance process.

LOCAL LEVEL

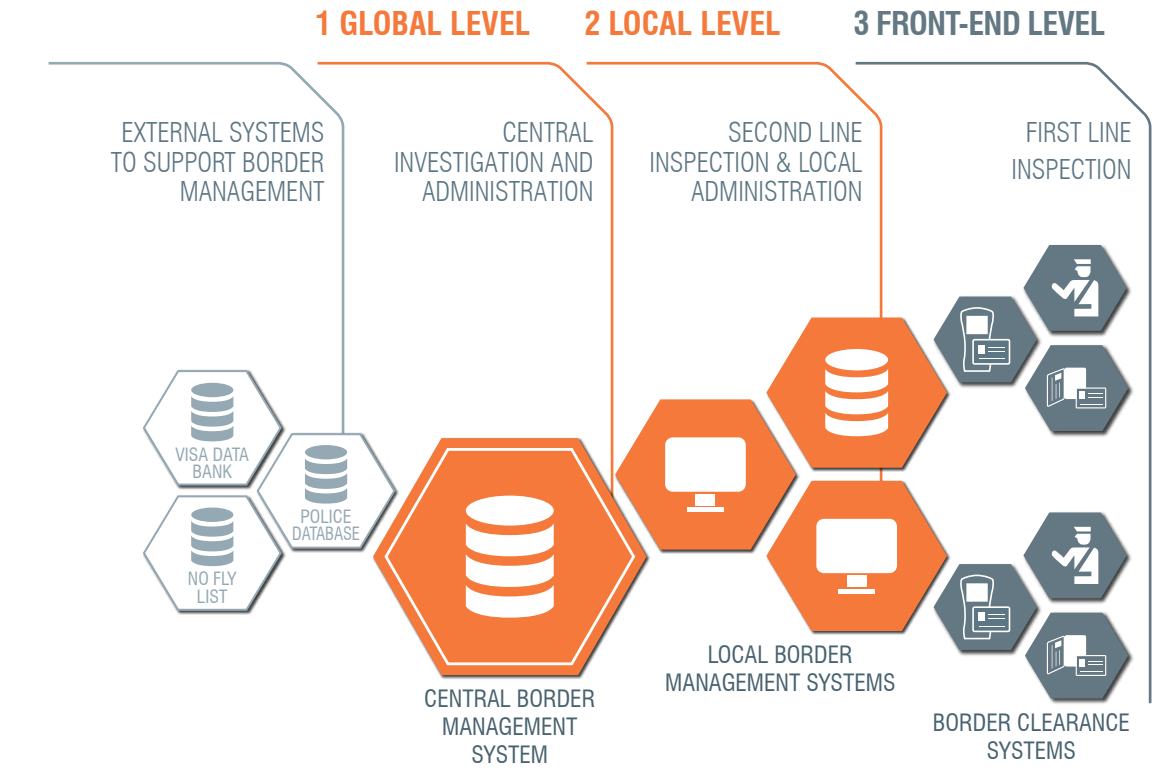
The local border management systems administrate the structures and information at country border points, e.g. at airports, sea-ports or land borders.

FRONT-END LEVEL

The border clearance systems aggregate software tools and peripheral devices to perform the verification process.

THREE-LAYER SOLUTION

The three-layer solution approach forms the technical basis for scaling all systems according to the capacity requirements and to creating standardized border clearance procedures at country border points. The soft- and hardware systems are modular components ensuring highest flexibility in the realization of projects. They enable solution updates due to technical modifications or changes in clearance procedures. The three-layer system hierarchically structures the data and border clearance applications and compiles the solution supervision functions in the central border management system.



LAYER 1 – GLOBAL LEVEL



CENTRAL BORDER MANAGEMENT SYSTEM

Applications for Supreme Border Authority

The central border management system incorporates sub-modules. They contain a central function unit, which allows for a full control of the nationwide border clearance process.

WORKFLOW MANAGEMENT SYSTEM

The system manages the border clearance routines for:

- Verification of document data authenticity
- Investigation of individuals by matching biometric features
- Investigation of visas or other external data
- Investigation of document authenticity

The verified data is provided (activated or deactivated) to front-end systems at country border points.

DATABASE AND INFORMATION SYSTEMS

The systems aggregate data relevant for border clearance from the local border management systems. A modern storage system collects and structures for example:

- Entry and exit information for the analysis of immigration-relevant aspects
- Border clearance track record information such as the MRZ extracted information, the system user and the inspection protocol

INTERFACE MODULE

The interface module operates towards system-internal and -external directions:

- In the system-internal direction, it connects local border management systems used at country border points with the central border management system, provides them with relevant data and inspection routines and receives border clearance information.
- In the system-external direction, it connects to visa information and identity databases and implements them into the border clearance process.

CENTRAL USER MANAGEMENT

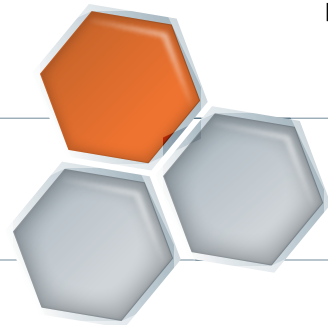
The system enables the definition of user groups and grants access to functions and data needed at the local border management systems. A controlled access to the workstations is provided for first and second-line inspection and for the background systems. Typical user groups are:

- Border point management team, having access to sensitive data and the related reporting functions
- Second-line inspection officers with access to enhanced inspection routines
- First-line inspection officers with access to basic inspection routines

REPORTING

Reporting functions visualize statistical information and match data with information stored in databases and information systems at border control points. The collected data supports the continuous improvement of the overall border clearance processes. The system provides information on:

- Entries and exits sorted by country and country border points
- Alerts on individuals who overstay
- Reports of system issues such as timeouts and non-functioning passports
- Traveler investigation



LAYER 2 – LOCAL LEVEL

LOCAL BORDER MANAGEMENT SYSTEMS

Applications for Superior Border Authority at Border Points

The local border management systems incorporate sub-modules, which enable a full control of the entire border clearance process at country border points.

WORKFLOW MANAGEMENT

The system manages all services required for the operation of a country's border points. It interfaces to the central management system and implements applications such as border clearance routines and monitoring for:

- Verification of document data authenticity
- Investigation of individuals
- Investigation of visas or other external data
- Investigation of document authenticity
- Usage of defined disaster scenarios

DATABASE AND INFORMATION SYSTEMS

The systems aggregate data relevant for border clearance from the front-end systems at country border points. A modern storage system collects and structures data such as:

- Entry and exit information as source for the analysis of immigration-relevant aspects
- Border clearance track record information such as the MRZ extracted information, the system user and the inspection protocol

EMBEDDING MODULE

The embedding module manages and connects relevant front-end devices such as:

- Manual border control systems
- Automated Border Control (ABC) systems
- Wi-Fi for handheld systems
- Monitoring systems
- Closed-Circuit Television (CCTV)
- Signaling systems

USER MANAGEMENT SYSTEM

The system enables the assigning of border clearance staff at country border points to defined user groups, relevant functions and data access. Typical user groups are:

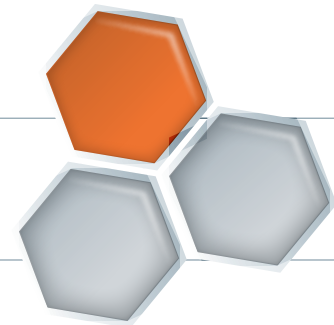
- Second-line inspection officers with access to enhanced inspection routines
- First-line inspection officers with access to basic inspection routines

An access control system allows for the authorization of access to basic or enhanced inspection routines, local sensitive data and the related reporting functions.

REPORTING

Reporting functions visualize statistical information and match data with information stored in databases and information systems at border control points. The collected data support the continuous improvement of the overall border clearance processes. The system provides information on:

- Entries and exits sorted by country and country border points
- Alerts on individuals who overstay
- Reports of system issues such as timeouts and non-functioning passports
- Traveler investigation



LAYER 3 – FRONT-END LEVEL

BORDER CLEARANCE SYSTEMS

Applications for First- and Second-Line Inspections

The border clearance process consists of various verification filters which are consecutively conducted to decide whether a passenger's entry is legitimate or not. Each filter is realized by software-based routines which extensively analyze the traveler's document and identity by using peripheral devices such as document readers, fingerprint scanners and face recognition systems.

If the analyses pass each filter, the verification is considered as fulfilled and the traveler is permitted entry. In case of document falsification, the traveler is routed to further inspection. Depending on the solution design, the traveler experiences the border clearance process as:

DESK-BASED SERVICE

The traditional desk-based service is supported by verification functions and peripheral devices to perform the verification process within a manual procedure at a service-counter. The border clearance process can be split up into first- and second-line inspection: The first-line inspection is performed at the desk with a standard verification routine set. In case of unacceptable results, the traveler is lead to the second-line inspection where a specially equipped workstation allows for further clarification.

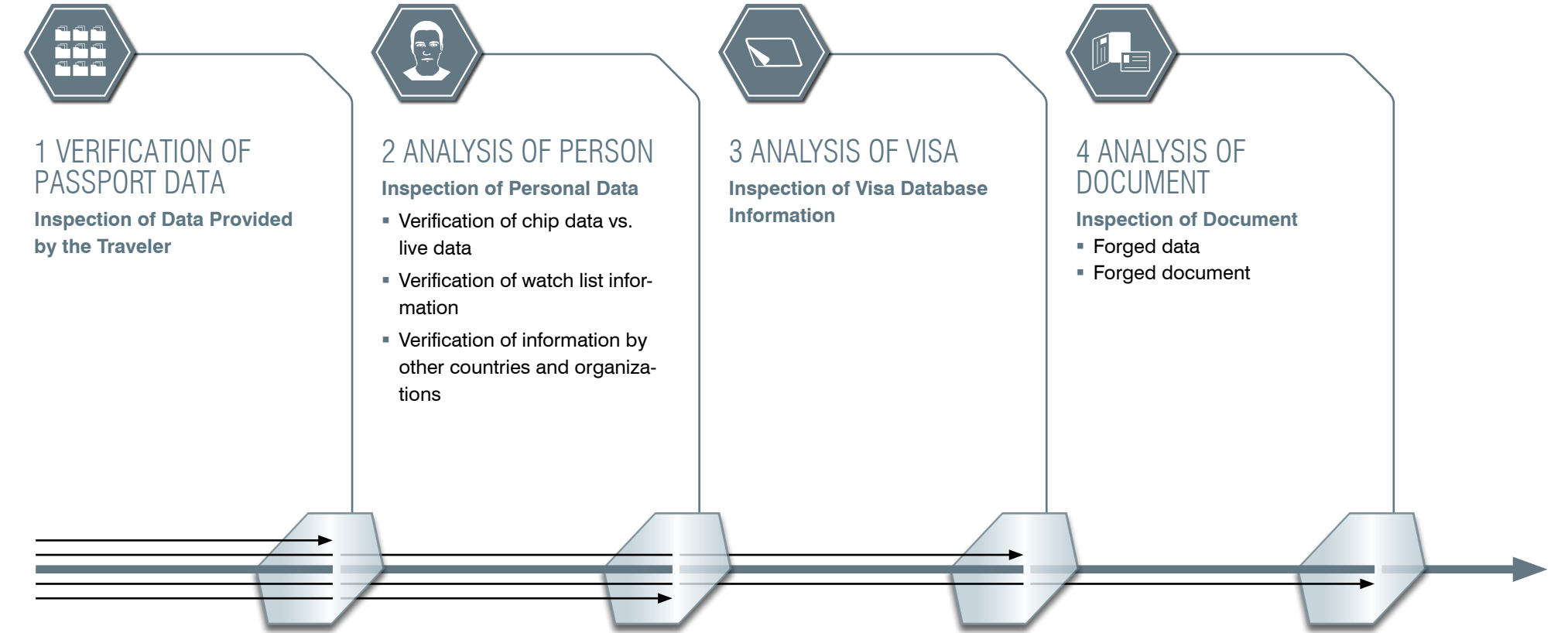
SELF-SERVICE

The self-service procedure is performed by using an Automated Border Control system with single or double door gate. Based on the requested border clearance process, a verification routine is created, enabling the automatic verification with regard to the four filters. The users are guided through the process where they have to present their documents and live data. The clearance process involves the local and central border management systems.

ON-THE-SPOT CHECK

The on-the-spot check is manually performed by officers using a portable verification device to check documents like ID cards and ePassports. Border guards equipped with this device can verify documents and individuals at any time without being limited to one specific location.

BORDER CLEARANCE PROCESS





EXEMPLARY PROJECTS

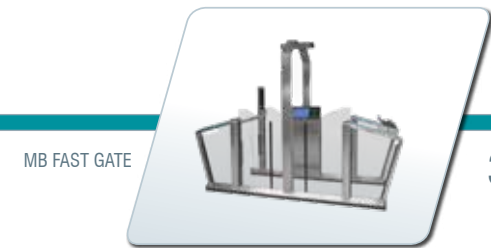
FREQUENT TRAVELER PROGRAM



ACCELERATED CLEARANCE

The frequent traveler program enables the accelerated entry for third-country travelers into the country: It issues the access solution and at the same time reliably verifies the traveler. To participate in the program, travelers register their demographic and biometric data at a point of service, for example an eTerminal, and are provided with a membership card containing their personal data. The program includes different services and is categorized in three levels – basic, middle and top level.

Similar to travel documents like ePassports, the card can be designed with high-security features according to international standards. Thus, the document is protected from counterfeit and fraud and the card can substitute the ePassport at all ABC systems included in the frequent traveler program. The three-layer system allows for the implementation of the frequent traveler program into several airports, land border points and seaports of the same country.



MB FAST GATE

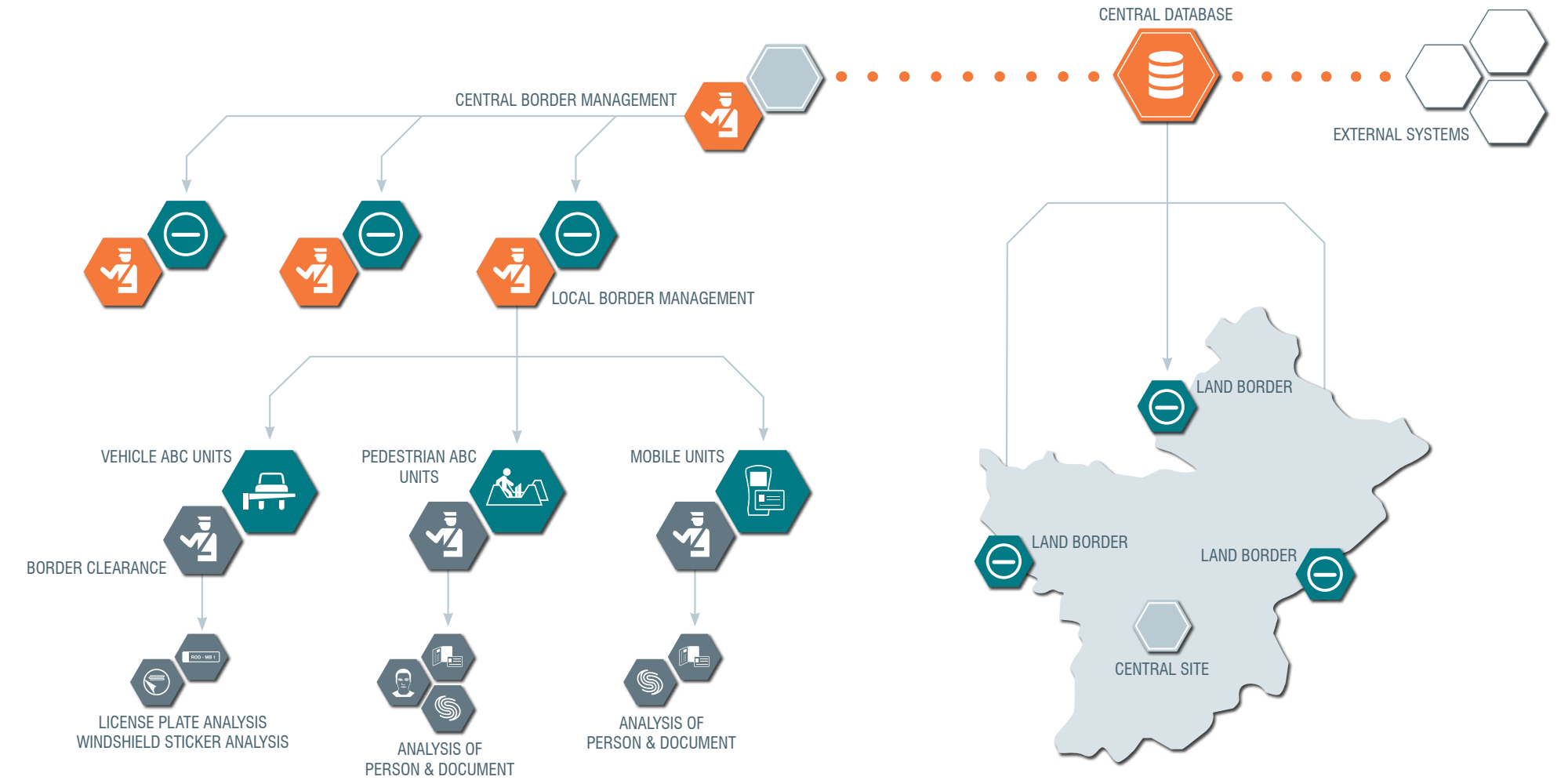
BORDER IDENTIFICATION & VERIFICATION



EFFICIENT CROSSING

The automated border control system allows for the fast and efficient identification and verification of vehicles and pedestrians crossing land borders. Registered vehicles receive RFID-tags which contain a chip with information about the holder, registered drivers and license plate. Upon arrival at the border, cameras capture the license plates while ultrahigh frequency devices read out the chip and match the data with the database. If more than one person is in the car or a case of falsification is detected, the vehicle is directed towards second-line inspection and manually checked.

Non-registered vehicles are randomly checked by inspectors by means of handheld devices. Thus, the efficient and secure identification and verification of documents and travelers is ensured. For pedestrian travelers, ABC units are installed which verify the eID card or ePassport and match the biometric data (face and fingerprint) with the registered data. In case of pre-registration, the ABC systems can also be used for customs clearance. Upon arrival at the border, the windshield sticker is read out and matched with the database of customs. In this way, the vehicle and the registered goods can smoothly be verified.



MB Handheld Verification Device



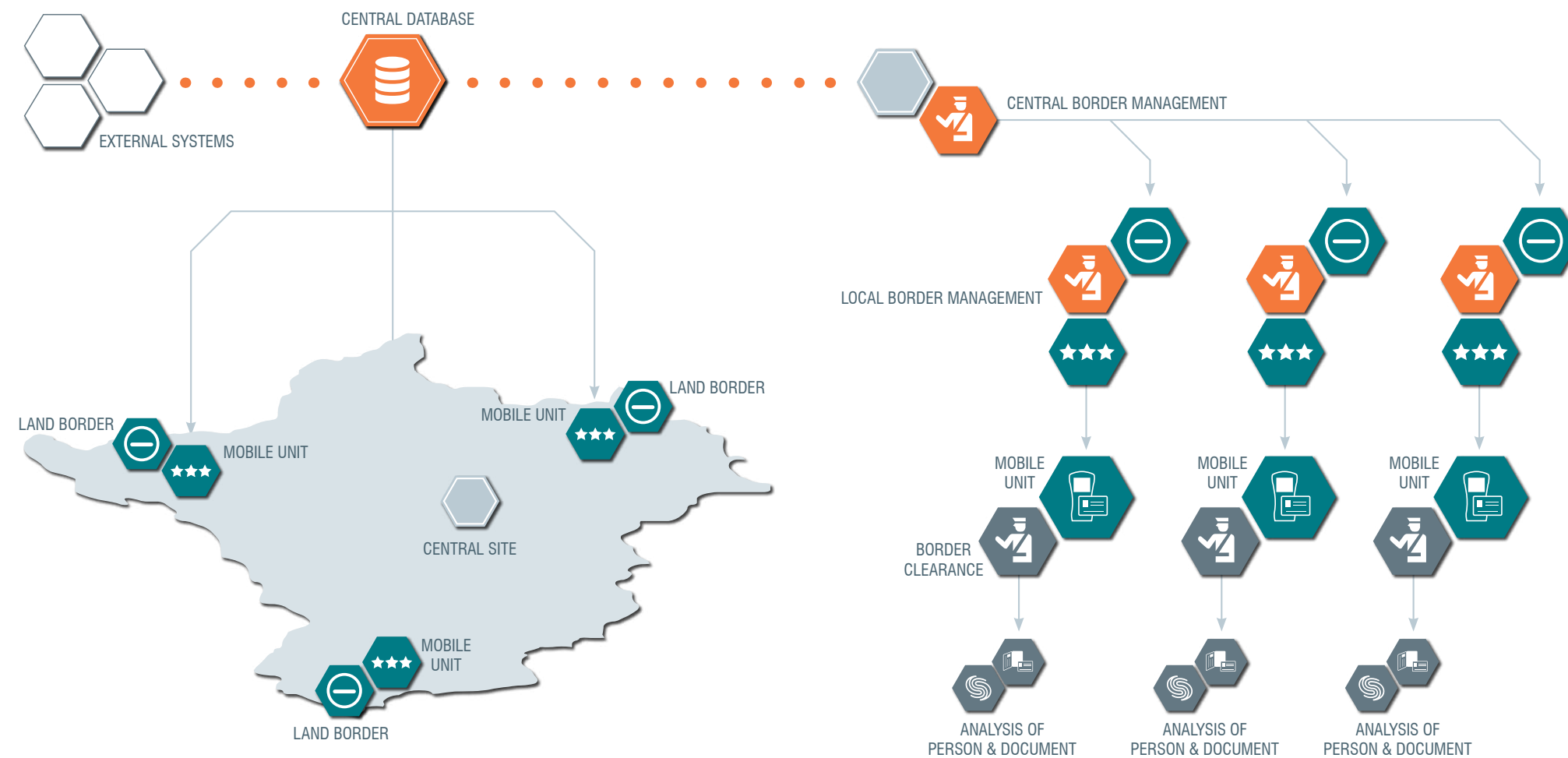
MOBILE IDENTIFICATION & VERIFICATION



FLEXIBLE AUTHENTICATION

Outside specific border crossing points, mobile verification devices enable the most flexible identification and verification of individuals and documents. Officers equipped with devices randomly inspect passing vehicles when patrolling along unsecured or lightly secured orders, at second-tier borders, at seaports, railway or ferry traffic checkpoints. These random routine checks are performed with regard to illegal migration and expired visas, but also to verify the documents and identify the individual.

During the inspection process, the handheld or getID verification device reads out the MRZ, thus verifying the document. In a second step, the device connects to the local management system to transfer the data which is then matched against national and international watch lists as well as Interpol and Schengen databases, entry and exit systems, and visa systems integrated in the central management system. Natives can additionally be verified by reading out their biometric data stored in the embedded chip and matching it with the live data from the fingerprint reader.



MB IDVERSO® FASTLANE

THE FUTURE OF AIRPORT TRAVELER MANAGEMENT

MB IDVERSO® FASTLANE guarantees the efficient and reliable administration of passenger and baggage handling, border control and boarding. Based on the autonomous operation of each single process step by the passenger, this highly sustainable solution ensures an optimized process flow. State-of-the-art technologies perfectly meet the demands imposed by the constant increase of passenger volumes.

Based on the system of biometric data processing and management, MB IDVERSO® FASTLANE combines three sub-processes: Automated Border Control, on-the-fly security systems and self-boarding systems without any physical barriers. To ensure the most efficient use of these components, a comprehensive cooperation between governmental authorities, airport operators, airlines and the solution provider is essential.

An individual token, which refers to a dataset of enrolled and process data, functionally connects the separate units. The dataset consists of a combination of demographic and biometrical data such as face, fingerprint and iris, as standardized by ICAO. The token is temporarily stored in the airport's background system. The data is used to validate the traveler's identity throughout the whole process on all biometrical interfaces. During the automated FASTLANE process, the passenger autonomously performs the defined process steps:

Step 1: Self-Enrollment & Check-In
The passenger enrolls at a common use self-boarding kiosk which reads out the boarding pass and matches the information with the data stored on the ePassport. With the personal and biometric data provided by the passenger, the identity authentication is performed and the temporary token is created.

Step 2: Operator-Assisted Enrollment
In case of operating errors or technical problems at the self-boarding kiosk, an additional service terminal is provided. This is where service staff assists passengers with the enrollment and check-in.

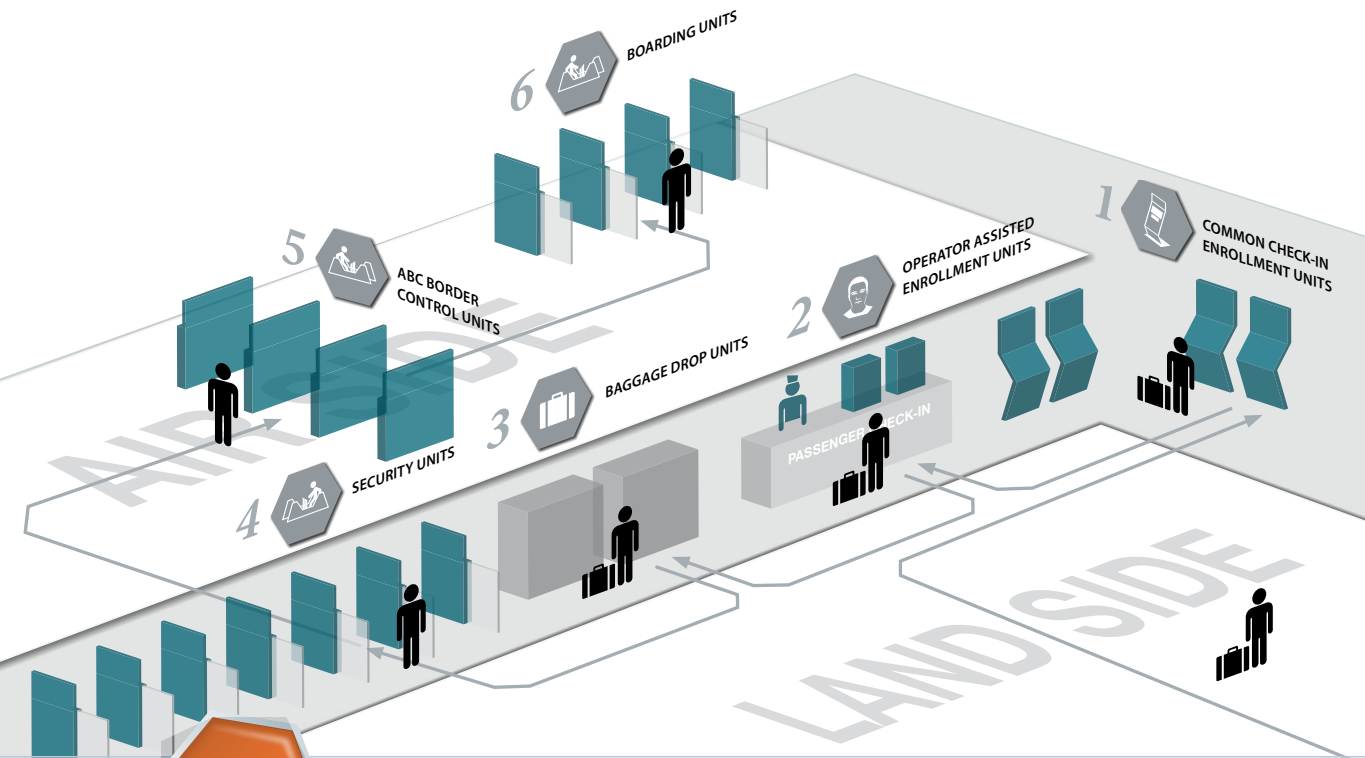
Step 3: Baggage Drop-Off
Specific self-service units are provided for the baggage drop-off. The background system identifies the passenger by matching live data with the temporary token, and processes the luggage data. The luggage is equipped with a physical token and the data is added to the enrolled passenger's information dataset.

Step 4: Security Check
The security units separate the land side from the air side. Once travelers pass through the security check, they are automatically identified and the status "passed security check" is added to their datasets. Within the air side, the

temporary token allows for the passenger's automatic authorization to use duty-free shops, lounges, as well as premium- and VIP-services.

Step 5: Border Control
At an ABC unit, the border crossing is performed within the air side. The passenger's biometrics are captured and matched with the virtual token for the reliable identification. Secondly, the data is matched with international watch lists in order to identify criminal or high-risk passengers. After successful verification, the passenger receives clearance for entry.

Step 6: Boarding
Upon the passenger's arrival at the boarding unit, the background system automatically captures the face biometrics and matches them with the virtual token. The passenger can instantly pass the unit without delay and the dataset referred to by the token is enhanced by the status "on board".



MB Single Gate Solution



MB FAST GATE

Fully-Automated Border Control

MB FAST GATE is designed according to the Frontex best practice technical guidelines for ABC systems. It combines modern, cost-efficient design and state-of-the-art technology to both accelerate and secure border control. Based on a user-centric approach, MB FAST GATE supports all eMRTD, ePassports and eID cards. It enables individuals to perform a fully-automated border crossing in a smart and rapid way.

Due to its modular hard- and software architecture, MB FAST GATE permits major adjustments: According to the individual project's requirements, individual elements, for example sensors, can smoothly be replaced or extended. Due to universal interfaces and a highly versatile structure which supports all known ABC topologies, the gates can flexibly be integrated into any given environment.

Most importantly, MB FAST GATE performs the high-speed, multi-biometric identity verification of individuals. ID documents are checked electronically and optically with regard to completeness, validity, correctness and holder authenticity in a fully automated way. Live data is verified by matching it with the data stored in the embedded chip and on the document surface (autarkic mode), or with external databases such as the national database and watch lists (integrated mode). Moreover, MB FAST GATE features the automated reporting of all border crossings and logging for quality assurance.

Security Against Forced Access

Due to its modular concept, MB FAST GATE achieves highest security standards. It allows for the flawless combination with online video surveillance systems and various sensors for security integrity. The comprehensive verification process of individuals and documents

includes numerous measures to avoid any case of manipulation or fraud:

- Measures against identity and document forgery - including the detection of document manipulation, optical and electronic document forgery and biometric presentation attacks
- Physical security measures against forced access
- Vision systems (for the detection of double persons and forgotten items) and anti-tailgating measures
- Security checks of forced access in the eGate workflow such as authorization checks, document verification, the background system (query of warrant database) and biometrics





MÜHLBAUER ID SERVICES GMBH

Josef-Mühlbauer-Platz 1 | 93426 Roding | Germany
Tel.: +49 9461 952 0 | Fax: +49 9461 952 1101
Mail: info@muehlbauer.de | Web: www.muehlbauer.de

