

# **MB IDVERSO**<sup>®</sup>

### BORDER MANAGEMENT SOLUTIONS









# COMPANY

## **COMPREHENSIVE SOLUTIONS**

#### Single-Source Technology Partner

Mühlbauer Group is the only globally acting single-source provider for end-to-end production of solutions and systems for the smart card, ePassport and semiconductor industry. We incorporate significant competence in providing optimized and state-of-theart technology as well as customized equipment. Our products merge the main three factors for our customer's success story:

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

#### **Business Unit TECURITY®**



Mühlbauer specializes in innovative one-stop solutions encompassing the production, personalization and issuance of ePassports, ID cards and other card related security documents, and fully automatic border control systems. The business unit TECURITY<sup>®</sup> bundles the extensive know-how of the development of tailor-made security solutions. In the last 30 years we have been intensively involved in over 300 government related ID projects across the globe.

#### **Business Unit Automation**



More than 100 different standard and customized products and intelligent software solutions for data enrollment, border control as well as personalization and production management are the core of the business unit Automation. The division is responsible for the development and manufacturing of Mühlbauer technologies. In addition to systems used for high-quality document production and personalization in high-end security products, we manufacture one-stop turnkey solutions for industrial image processing of cards, coins and banknotes, tubes and other products. Moreover we develop and produce innovative systems such as micro-chip die sorting, flexible solar cells or carrier tape equipment for specific niche applications in the semiconductor back-end area (semiconductor related products), as well as labeling and marking systems for traceability of electronic components (traceability).

#### **Business Unit Parts & Systems**



Mühlbauer's Parts & Systems 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 One of the effects of the globalized world is the constant increase of travel activities worldwide. The annual rise of roughly 3.7% in passenger volumes will result in a total of 7.2 billion flight passengers by 2035 (Source: IATA).





Management organizations and authorities at airports, seaports and land border control points are in need of solutions to cope with this development whilst at the same time preserving security standards. Passenger satisfaction depends on the facilitation of border crossings by speeding up the processing despite the higher volumes and enabling a more convenient traveling. Due to international threats and trans-border crime, however, security measures have to be enhanced in order to quickly and reliably verify travelers' identities. Future border management systems therefore must manage to quickly, conveniently and cost-effectively handle lowrisk passengers while reliably identifying and separating potentially high-risk travelers.

#### Threats and Challenges for Border Clearance



#### **Latest Technologies**

In order to cope with these trends, establishing latest technologies has become essential:

- Automated Border Control systems (ABC systems) efficiently perform the border control process thus expanding the control capacities within a limited investment.
- Innovations like 3D face recognition allow for an even more accurate authentification.
- The increasing amount of ePassports and next generation eMRTDs serve to enhance security and facilitation during the issuance process and the use of the document.
- Advance Passenger Information systems are integrated to capture extended data of the traveler and receive the information well in advance of his arrival.
- The border management systems match the data with international watch lists informing about stolen documents or other criminal background.

#### Effects of Automated Border Control Systems

One of the key benefits of ABC systems is the increased capacities for border clearance by enabling the more efficient use of the existing - and in most cases optimized - infrastructure. Instead of effecting cost intensive measures such as the expansion of the terminal infrastructure, the investment in ABC systems allows for a faster and more efficient processing of passengers, leading to decreasing queuing times and lower levels of congestion with given amount of staff and space. Cost reductions are effected by the installation of self-service checks instead of desk-based checks. Additionally higher verification standards are implemented for the traveler's identity and his travel documents, including the matching with biometric information.

Introducing Integrated Border Management A first step in enhancing facilitation and efficiency is the installation of Automated Border Control systems. In order to ensure effective processing next to highest security long-term, they integrate global information systems and latest standards of ABC solutions, and comply with international regulations and guidelines. Integrated Border Management systems are equipped to include any relevant information systems, manual inspection and next generation ABC during the border crossing process, following standards leading to global interoperability and security.

#### **Global Interoperability**

Whereas border management systems ensure facilitation and efficiency nationally, worldwide security can only be enhanced by their abilities to interoperate globally with 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 must be designed as to be able to process different kinds and generations of travel documents according to the international standards. 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

POLICE

Electronic machine readable travel documents (ePassport, eVisa or any other electronic ID document accepted for traveling purposes) allow for the reliable identification and verification of the traveler. The international specifications for eMRTDs, according to Doc 9303 published by ICAO, ensure that documents complying with these standards can be read with any suitable device or ABC unit, thus enhancing security and facilitation throughout the whole processing. Next to the MRZ (Machine Readable Zone) which has been established to simplify the capturing of the document information, the eMRTD holds a storage chip containing the holder's personal and biometric data. By using 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. Whereas cur-

rent ePassports are limited in their functionality, the new LDS 2.0 is an enhanced eMRTD with chip applications which are able to hold eVISA and advance passenger information in order to secure fast access, and can serve as token for temporary travel records.

#### eVISA

The visa has become an essential part of the border control process, since it is getting increasingly important to receive further information on the traveler well in advance of his arrival. Border management solutions therefore have to efficiently integrate the visa into the control process to meet the overall challenges of increasing traveler volumes but also allow for facilitation for the passenger. Especially eVISA form a convenient and efficient alternative to the standardized visa application procedure where the traveler has to apply at embassies in advance or at least has to queue at ports of entry where visas can

be issued. The document contains information on the applicant, the duration and the purpose of the stay, as well as a MRZ, which has to be read separately from the verification process on entering the country, leading to longer processing times. In order to render the process more efficient the applicant can apply for an eVISA online at a web portal by transmitting his personal data which is 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. thus significantly reducing processing time and enhancing passenger facilitation.

#### **Visa Information Systems**

Visa information systems serve the facilitation of visa applications and support border clearance authorities to avoid fraud and – in case of the Schengen states – "visa shopping" (applying for visa to further Schengen states although a first application has already been rejected).

The 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 intending to enter the country thus enabling authorities to quickly and easily verify the identity of the visa holder during the border clearance process. The verification is carried out by reading the traveler's fingerprint and matching it with the data stored in the visa information system ensuring that the person who applied for the visa is the one holding it.

#### **Advance Passenger Information Systems**

In order to cope with the increasing international challenges and threats, Advance Passenger Information systems have been introduced to provide information on the travelers well in advance before they enter the country. During check-in the personal data of the passenger, together with his 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 who match the data against databases and watch lists, enabling the facilitation of border control and avoiding illegal entry.

#### Watch Lists and Databases

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

#### **Examples for Watch Lists are:**

- Interpol Terrorism Watch List: Informs on fugitives and suspected terrorists
- Interpol Stolen and Lost Travel Document (SLTD) database: Links missing travel documents to fugitives
- EdisonTD: Holds genuine examples of 3000 documents from 206 countries
- Dial-Doc: Shares new counterfeiters among G8 countries
- Schengen Information Systems (SIS and SIS II): Hold information on wanted and observed persons, missing persons, unwanted persons and objects, and items such as weapons



# MILESTONES OF BORDER MANAGEMENT

<< MRZ <<<< 000123456 <<

# **1980** STANDARDIZATION OF MRTD

ICAO standardizes traveler documents with the release of ICAO 9303 W/MRZ standard. The first MRTD is introduced one year later, integrating the personal data in a format to be automatically read out.



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.



The first ePassport is issued including an embedded chip containing the personal data and biometrical information of the holder.



# **EU 1995** INTRODUCTION OF SIS

The Schengen States launch the Schengen Information System (SIS) for the automated distribution of information about wanted individuals. It is enhanced by biometrical information in 2013 (SIS II).



# 2002 LAUNCH OF INTERPOL WATCH LIST AND DATABASES

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





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

# 2014 INTRODUCTION OF SAC

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



The next-generation ePassport LDS 2.0 contains further applications such as eVISA and advance traveler information. First reference implementations are planned for 2015.

# 2009 EAC BECOMES MANDATORY IN THE EU

The Extended Access Control (EAC) system adds to the BAC by verifying the genuineness of the chip and protecting the access to the more sensitive biometrical data stored in the chip.

# **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.

## **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 functions and procedures related to the border clearance process in order to help management organizations and authorities (e. g. contracting states implementing the standards) to optimize border control, and to achieve and preserve highest security standards, interoperability and effective law-enforcement.



### **RESOLUTION 1373**

The events of 9/11 caused nations worldwide to focus on the importance of comprehensive border control, initiating the current developments of 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 actions 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, such as 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. Doc 9303 is constantly enhanced with new specifications such as next generation eMRTDs (LDS 2.0), containing latest security features and technologies for secure data storage in order to prevent counterfeiting and fraud.





The code defines key rules for the management of borders to be followed by the Schengen member states in order 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 moreover 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 the soft standard for the design, the deployment and the operation of ABC systems. They define the benefits and basic requirements (including key components such as physical barriers, document readers and biometry capture devices) based on a coordinated exchange of experiences, in order to ensure efficient border crossing and highest security standards. The focus of the guidelines is on ABC systems used by EU citizens with ICAO Doc 9303 compliant eMRTDs.



SmartS envisions an uninterrupted passenger flow through security checkpoints at airports. Security resources are allocated and optimized, enabling a real-time risk assessment without inconveniencing passengers unless potential threats are identified. The program signalizes the development towards comprehensive solutions dealing with increasing passenger volumes, whilst ensuring 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

In order to provide the MB IDVERSO<sup>®</sup> border management solution a three-layered software model has been created, which 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 such as airports, seaports or land borders.

#### FRONT-END LEVEL

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

# 20|21



The three-layer solution approach forms the technical basis to scale all systems according to the capacity requirements and to create a standardized border clearance procedure at country border points. The soft- and hardware systems are created as modular components ensuring highest flexibility in the realization of projects and enabling solution updates due to technical modifications or changes in clearance procedures. The three-layer system structures the data and border clearance applications in a hierarchic format and focuses the solution supervision functions on 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, which enable a full control of the nationwide border clearance process by a central function unit.



The system manages the border clearance routines for:

- Verification of document data authenticity
- Investigation of individuals by matching the 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 border clearance relevant data from the local border management systems. A modern storage system collects and structures data such as:

- Entry and exit information serving 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





#### INTERFACE MODULE

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

- In the system-internal direction it connects local border management systems applied 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 systems such as 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
- Inspection officers of the first line inspection with access to the basic inspection routines

#### 

Reporting functions serve to visualize statistical information and to 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 the services needed for the operation of the country border points according to the defined requirements. 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 by matching the biometric features
- Investigation of visas or other external data
- Investigation of document authenticity
- Usage of defined disaster scenarios

#### DATABASE AND INFORMATION SYSTEMS

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

- Entry and exit information serving 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 connects the frontend devices such as:

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

It manages the devices and provides the relevant data.

#### 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 the 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 functions serve to visualize statistical information and to 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 3 – FRONT-END LEVEL

#### **BORDER CLEARANCE SYSTEMS**

Applications for first and second line inspections

The border clearance process essentially consists of various verification filters conducted consecutively to reach a decision whether the entry is legitimate. Each filter is realized by software based routines performing extensive analyses of the document and the identity of the traveler by using peripheral devices such as document readers, finger-print 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 falsification, the traveler is routed to further inspection. Depending on the solution design the traveler experiences the border clearance process as:



The traditional desk-based service is supported by verification functions and peripheral devices in order 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 not acceptable results, the traveler is lead to the second line inspection. A specially equipped workstation allows for further clarification.

#### SELF-SERVICE

The self-service procedure is performed by using an Automated Border Control system (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 user is guided through the process where he has to present his document and live data, resulting in clearance. The clearance process involves the local and central border management systems.

#### SON-THE-SPOT CHECK

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







## 26 27



# EXEMPLARY PROJECTS

# FREQUENT TRAVELER PROGRAM



#### ACCELERATED CLEARANCE

The frequent traveler program enables the accelerated entry for 3<sup>rd</sup> country travelers into the country issuing the access solution whilst reliably verifying the traveler. To participate in the program, the traveler registers his demographic and biometric data at a point of service, such as an eTerminal, and is provided with a membership card containing his personal data. The program can be categorized in three levels (basic, middle and top level) including different services.

Similar to travel documents such as ePassports, the card can be designed with high-security features according to international standards, protecting the document from counterfeit and fraud, and enabling the use of the card as substitute for the ePassport at ABC systems included in the program. The three-layer system allows for the implementation of the frequent traveler program into several airports as well as land border points and seaports of one country.





# **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 containing a chip with information about the holder, the registered drivers and the license plate. Upon arrival at the border, cameras capture the license plates while ultra high frequency devices read out the chip and match the data with the database. If more than one person is in the car or in case of falsification, the vehicle is directed towards second line inspection and checked manually. Non-registered vehicles are checked randomly by inspectors using handheld devices ensuring the efficient and secure identification and verification of the documents and the traveler. For pedestrian travelers, ABC units are installed verifying the eID card or ePassport and matching the biometric data (face and fingerprint) with the registered data. In case of pre-registration the automated border control systems can also be used for customs clearance. Upon arrival at the border, the windshield sticker is read out and matched with the customs database verifying the vehicle and the registered goods.

# 32|33





# **MOBILE IDENTIFICATION & VERIFICATION**



#### FLEXIBLE AUTHENTIFICATION

Mobile verification devices enable the most flexible identification and verification of individuals and documents apart from specific border crossing points. Officers equipped with devices randomly inspect passing vehicles when patrolling along unsecured or lightly secured borders, at second tier borders in a certain distance from border crossing points, or at seaports, railway or ferry traffic checkpoints. The random routine checks are performed with regard to illegal migration and expired visas but also to verify the documents and to 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 and databases such 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

The MB IDVERSO<sup>®</sup> FASTLANE system guarantees the optimized process flow, based on the autonomous operation of each single process step by the passenger. New technologies, sustainable solutions and the efficient and reliable administration of passenger and baggage handling, border control and boarding meet the demands imposed by the constant increase of passenger volumes.

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

By using an individual token, referring to a dataset of enrolled and process data, the separate units are connected functionally. 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 background system of the airport and the data is used for the validation of the traveler's identity throughout the whole process on all biometrical interfaces. During the automated FASTLANE process the passenger autonomously performs 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 issues at the self-boarding kiosk an additional service terminal is provided where enrollment and check-in is performed with the assistance of service staff.

#### Step 3: Baggage Drop-Off

Specific common use 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 information dataset.

#### Step 4: Security Check

The security units separate the land area from the air area. Once the traveler passes through the security check, he is automatically identified and the status "passed security check" is added to the dataset. Within the air area, the temporary token allows for the automatic authorization of the passenger for the use of duty-free shops, lounges and premium- and VIP-services.

#### Step 5: Border Control

The border crossing is performed within the air area at an ABC unit. The passenger's biometrics are captured automatically and matched with the virtual token for the reliable identification. In a second step the data is matched with international watch lists in order to identify criminal or high-risk passengers. After verification the passenger receives clearance for entry.

#### Step 6: Boarding

On arrival of the passenger 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".







# SYSTEM ARCHITECTURE

## INTEGRATED BORDER MANAGEMENT

Integrated Border Management Architecture Mühlbauer's Integrated Border Management solution architecture is based on flexible and customizable software modules. The design is driven by today's border management challenges, international guidelines and programs such as ICAO's latest Traveler Identification Program (TRIP), and best practices. Prior to implementing Integrated Border Management, the basic specifications have to be determined:

- Which different types of borders shall be supported
- Which functions should be conducted at borders, e.g. manual or automatic traveler inspection, customs and goods inspection, etc.
- Which are the major objectives of the Integrated Border Management system, e.g. shall there be entry and exit registration for more secure and efficient traveler verification

Which are the dimensions of the border solution, e.g. which traveler volumes must be processed, which external information systems, interfaces etc. must be incorporated

The modular architecture is designed in order to provide tailor-made solutions for different countries and customers based on their individual regulations and requirements.

#### **Software Layers and Solution Components**

The different component layers allow for a broad range of solutions. Simple check points, border posts or more complex ABC solutions can be implemented as well as local or even global border management systems for securing airports, seaports and land borders nationwide. Mühlbauer's approach defines the basic layers and components connected by standardized and secured interfaces for highest security and system availability.

The bottom layer (local ABC system) of the architecture contains all modules required to set up ABC next generation systems for eMRTD and passenger verification. All software modules are securely integrated into the layer components representing functions such as controlling, local databases for logging all the transactions of manual inspections and eGates, PKI and certificate handling for document verification. Kiosk solutions can be provided as well as sophisticated monitoring systems.

The passenger layer of the local border management system covers a complete border management solution including extended interfaces to watch lists, API systems, Interpol's SLTD and other police databases as well as large data management systems for entry and exit data management and analysis. The general layer of the local border management system integrates the components, including sophisticated biometric identity management and connects them with the global layer for a nationwide solution.





CENTRAL BORDER MANAGEMENT SYSTEM

## **MB FAST GATE**



#### Fully Automated Border Control

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

DEVELOPMENT KIT Characterized by a modular hardware and software architecture the MB FAST GATE permits major adjustments. Individual elements such as various sensors can be easily replaced or extended according to the project requirements. Due to universal interfaces and a highly versatile structure supporting all known ABC topologies, the gates can be flexibly integrated into any environment.

The FAST GATE provides high-speed multibiometric 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 the FAST GATE features automated reporting of all border crossings and logging for quality assurance.

#### Security Against Forced Access

Due to the modular concept, the MB FAST GATE achieves highest security standards. It allows for the 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 manipulation or fraud, such as:

- · 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 GROUP

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

