TECHNICAL DATASHEET

SBMS

Secure Border Management System

The current scenario in the world where globalization and traffic between countries have increased dramatically, where illegal immigration, high criminal rates and terrorist threats become a major concern for governments, calls for increased public security. The fight against this issues demand a huge effort from immigration and police authorities in order to create a Secure Area within the geographical limits of the country. Our Secure Border Management System integrates the latest advances in security technology and provides to the immigration authorities a tool to

fight efficiently against these new threats. SBMS supports the new e-passports and e-visas as well as the automated verification of printed security features in all travel documents whether they are machine readble or still hand written. A variety of outstanding features like ICR recogntion of Entry/Exit Cards, 1:n face recognition and 1:n fingerprint comparison against a wanted list make it an outstanding solution.
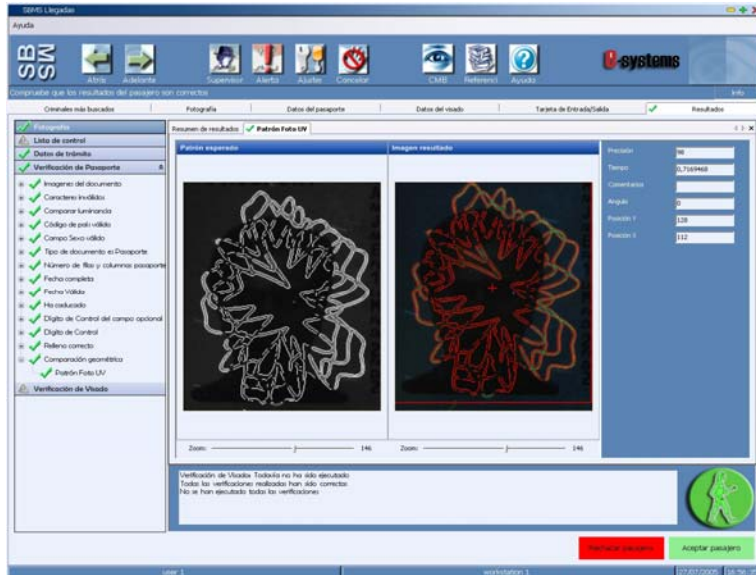
Key Features

Architecture

The system architecture has been carefully designed from scratch to benefit from the latest trends in software development:

- Service Oriented: A modular service layer, based on messages, is used to glue the system together. This flexible design allows maximum extensibility without outgrowing the initial design.
- Rich Client paradigm: The intuitive and powerful user interface of desktop applications; the ubiquity and easy deployment of Web-based applications.
- Truly scalable: From a single machine setup to thousands of simultaneous users and an enterprise-grade cluster of servers. From a local network to later embrace the Internet or a virtual private network.
- Developed on the best-fit platforms: Microsoft.NET for the best end-user experience, robust and scalable Java's J2EE on the server side.
- Based on standards. For the best interoperability between different platforms and systems.

Data Capture

Capture of textual information from the document via the Machine Readable Zone (MRZ) and the document image in all different lights available (UV, Infrared, 3M laminate, Normal).

Automated capture of data from the RFIP chip of the e-passport or e-visa in one single step during scanning of the data page.

Manual capture of passports that are not machine readable yet. Smart fields support the quick data entry by default values, preset values and drop down boxes.

All data captured from the document is checked against the control list and the security features against the template stored in the database.

Face Verification

Consists of the face capture function of travelers, allowing the operator to take several images and select the image that it is most appropriate for the verification process.

The system performs a Live Quality Control of every picture taken, informing the operator of the overall quality of the image and suitability for Facial Recognition.

Additionally the system performs a 1:n search against a control list and a 1:1 against the image retrieved from the document, if it is an e-passport.

Document Verification

This module provides complete and automated verification of travel document images with its security features stored in the database for the specific document. All verifications are performed automatically analyzing images and comparing security patterns in various light sources.

Additionally all information related to MRZ and information in the Visual Inspection Zone are read and compared using a state of the art OCR engine.

All RFID chip data are properly verified using the respective encryption keys and certifying thereby the authenticity of own document as well as the travel documents of other countries.

VeriDoc is also available as an independent application and as a SDK.

Exception Handling

Enables the supervisor to finalize the transaction when the system rejects the document or the person has some restrictions to exit or enter the country. Usually that functionality is invoked by the operator who passes on a transaction to the supervisor/secondary inspection and there, usually in the back office, the exception handling is performed.

Database Replication

This module replicates critical information from the headquarters to all ports of entry and vice versa. It incorporates a complete set of tools and applications developed for monitoring and administering the replication procedures, guaranteeing the data integrity among all database systems.

Entry / Exit Card Recognition

Countries that redesign their Entry/Exit cards so that they can be scanned by the passport reader can perform data capture and ICR processing of the handwritten information from the entry/exit cards.

Not recognized characters are highlighted and the cursor is pre-positioned at those characters.

Correction of not recognized characters by the operator is supported by displaying the card and displaying the respective enlarged image area for easy reading and correction. The operator can perform the capture right away of can perform the correction later in a batch process.

Visa Processing

A module that is invoked automatically when a visa is mandatory for that traveler. A specific database table holds the information which nationalities need a visa. The functionality supports the automated reading of e-visas as well as the scanning of MRZ visas and the manual recording of visa relevant fields.

Most Wanted List

The Most Wanted List is a subset of the Control List which can be accessed by operators of the SBMS at any time during the workflow. Mandatory the most wanted will be displayed at the startup of the application.

The operator can view the photo and read the description of the most wanted person to get familiar.

New entries in the most wanted list are marked in the overview to attract the special attention of the operator.

An administrator can select within the control list the most wanted persons in order to enable them for this module.

Fingerprint Verification

The Fingerprint Verification module consists of a fingerprint capture function and the 1:n search against the control list.

If the travel document contains a 2D barcode with a fingerprint template or an RFIP chip with a fingerprint image, then a 1:1 comparison between live finger and stored document finger can be performed as well.

The module permits to setup any numbers of fingers to be captured and it performs automatically quality assurance of the live image to assure the usability of the fingerprints taken

Online Help System

SBMS has a comprehensive online Help System which provides a set of documentation in an easily accessible way. When accessed, the Help System will open in a new Browser-window using Internet Explorer 6.0 or a compatible Internet Browser like Opera, Mozilla, Netscape, etc.

The Help System will start with an introduction page of how to use the Online Help system. Afterwards, the Help will be self-explanatory and will guide the user through the documentation to the specific point of interest. Alternatively, a more proficient user is able to navigate directly to the Help-system using the contents, index or search menus.

Bookmarks are created to help the user navigate efficiently through the help document, in order to provide them with quick and comprehensive help. A supplementary printed version of the extensive Online Help serves as the User Manual.

Reference

The Reference Module delivers for each document in our database high resolution images with its security features description in an easy readable and scrollable format.

All Operators of the SBMS have the ability to invoke that module anytime to refer to it in case of any suspicious travel document they deal with.

Functionality

Arrivals

The Arrivals application consists of several mandatory modules and various optional modules as outlined before. It is the most complex application that is implemented and this application is usually used to demonstrate the capabilities of the SBMS.

Description

The purpose of this application is allowing the officer at the arrival gate to
- Visualize the Most Wanted Criminals
- Perform a biometric verification (Fingerprints and/or Iris and/or face recognition)
- Capture the information of the travel documents handed over by the traveler
- Verify the document authenticity and security features
- Capture the image of the Entry card
- Applying ICR process to the just captured image of entry card and perform the reject/repair operation
- Search for control list hits
- Handle of exceptions encountered

High-level list of functions

- Allow the officer to scan and rescan travel documents (including special documents such as visas, work permits, etc.).
- Automatically alert the officer if the passenger is a minor or requires a visa to enter the country

- Allow the officer at the gate to call the supervisor if it's needed.
- Automatically read the data of documents complying with ICAO specification.
- Allow the user to manually key in the information of non-ICAO documents.
- Automatically perform a verification of the security features of documents
- Display all details from the verification of document security features
- Provide specific control list check.
- Allow the officer to scan the Entry/Replacement card.
- Allow the officer to do the ICR and Reject/Repair of the Entry/Replacement card data.
- Allow the officer to notify the supervisor if there is a hit in the control list or failure during VeriDoc check.
- Enable the officer to capture and verify biometric information
- Display of Control List Hit if founded
- Display transit global result (Can Go, Not Go)

Departures

The Departure application can be identical to the Arrival Application or can be a subset of modules only, based on the business rules for each country.
For instance can a traveler processed by simply scanning his exit card. The transit database contains the pending record, all searches can be performed and the record is closed. In this scenario the traveler does not even have to present his travel document.

System Access Security and User administration (SAPS)

This independent module manages centralized the user administration, roles and access rights to the different modules part of the system.
The application contains a database which is stored at the headquarters in the same server as the SBMS central database or in its own server. SAPS it is an independent system that is integrated into SBMS to manage all user, stations and access right information.
The SAPS Administrator is in charge of the administration of the Access Security to the entire system. This task is performed using the SAPS administration application provided with the SBMS system.

Control List Management

This application enables the user to introduce data to the control list tables to check textual information of the document. The control list holds all information related to people that can not enter or exit the country, as well as stolen documents.
The control list can be linked to different official sources of information provided by the local authorities.
Only the users with the right permissions can access the Control List Management application. A workflow of authorizations can be needed also to commit the changes in the control list. For example, a control list administrator might have permissions for modifying the control list; however a revision from the control list supervisor is needed afterwards before the changes are actually active in the database.

Reports

Allow a supervisor to generate administrative reports, such as passenger lists, transactions by officer, etc. These reports can be
- Local reports: performed at the port of entry (POE), containing information relative to this POE
- Central reports: performed at the headquarters, containing global information of all the POE.

Frequent Traveler Gate

This is an unmanned control point whereby passengers will be automatically identified using their biometric travel document, and consequently allowed to pass through in accordance with a verification process.

Upon arrival at the gate, the traveler will submit his/her travel document to be scanned. The gate will automatically read all of the machine readable data on the document including the biometric data. The traveler will then look into a camera to allow the gate to perform face recognition, and will also place his finger upon a fingerprint scanner. The travelers face and fingerprint images will be analyzed against the biometric information stored on their travel document. Upon a positive match, the passenger will be allowed to proceed if they are in the access control list for that gate (if such a list has been specified).

Additional security features of the gate may include iris recognition, and the ability to detect if more than one person is accessing the gate. The latter of these two will help to detect if a passenger is being coerced by another party to gain access. Furthermore, transit data will be obtained from the gate, stored in the SBMS transit database and the passenger details will be checked against the control list.

SBMS Management

This tool provides the functionality needed by the system administrator for configuring the system with the different modules and applications that will be used. SBMS is able to adapt to any kind of organizational infrastructure and workflow.

Access rights to the applications can be customized depending on the organization, for example, the supervisor applications can be available only to one user in every port of entry, or can be available to every operator.

Different modules can be included depending on the infrastructure available on the POE, for example, Face Recognition Module can be activated only for the border control gates in airports. S BMS management application allows the administrator to configure the system for the needed functionality at every POE and provides flexibility to modify these settings on run-time in case it is needed.

Technical Data

Software Architecture

The system architecture follows the SOA paradigm: Service Oriented Architecture. This design methodology helps to build flexible solutions that can easily been upgraded and maintained. We are using all standards to maximize the interoperability and keep the architecture up to date: Web Services technologies, WSDL, SOAP, XML, XML Schema and others.

From a technical point of view, the SBMS system consists of the following building blocks:

The rich client applications

They are .NET applications built over a common framework called SBMS Agent that is responsible for all the interactions with the service layer. They exploit all the grandeur of the User Interface on the Windows platform to offer an unparalleled user experience.

SBMS Server

SBMS Server is a J2EE 1.4 application running on the Oracle Application Server. It is possible to scale it either vertically, running multiple application servers on a single machine, or horizontally, were the application is seamlessly distributed between different machines on cluster or over the network.

The SBMS Service layer services the client applications and is built upon Web Services and Web authoring technologies (WS-I Web Services Basic Profile 1.1, SOAP 1.2, WSDL, XML, XML Schema, WebDAV). It has been designed based on a messaging paradigm, whereby everything is a message. These messages are written in XML and are checked against the grammar contained on an XML schema for validation and completeness. This data on transit can be signed and encrypted by using Web Services Security (WS-Security).
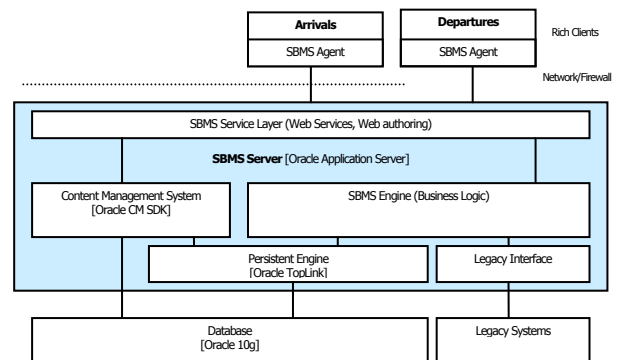
The Content Management System subsystem is based on Oracle Content Management SDK, included on Oracle Application Server. This subsystem is highly optimized to handle binary content.

The Persistent Engine subsystem, based on Oracle TopLink, is a layer between the business objects to data stored in a relational database. TopLink is an Object Relational Mapping (ORM) tool that allows clean application of object-oriented design, analysis, and programming techniques to the business logic whilst hiding the specifics of dealing with the relational system.

The Legacy Interface is a placeholder for different integration scenarios. The architecture is designed for being as open as possible and we support integration at the data store level by JCA (Java Connector Architecture), JDBC (Java Database Connector) and TopLink. Finally it can easily integrate with third-party Web Services, which is the preferred way.

The server side infrastructure is supported by Oracle products: Oracle Application Server and Oracle Database. They are supported on many combinations of hardware platforms and Operating Systems. SBMS Server is a J2EE 1.4 fully conformant application and can be easy ported to any other J2EE Application Server such as IBM Websphere or BEA Weblogic. Finally, Oracle TopLink provides us with portability between databases.

Technical Infrastructure

- Client Environment
  - Windows XP
  - .NET Framework 1.1
- Server Environment
  - Oracle 10g DBMS
  - Oracle Application Server 10g
  - Supported Operating Systems: Windows Server 2000/2003, Solaris and Red Hat Linux
  - Supported Hardware Platforms: Intel x86, Itanium 2, AMD64 and Sparc.
- Development Tools:
  - Microsoft Visual Studio .NET
  - Oracle JDeveloper
  - Matrox Imaging Libraries for image manipulation
- Digital camera for Face Recognition
- Travel document readers: IDStar 4054, SFO Authenticator 200, AR CLR233 RFID