A Short Resume of Romanian Electronic Passports System - ePASS

Claudiu Horăţiu JUDEA
Information Technology Security Master
Bucharest Military Technical Academy
ROMANIA
horatiu_j@yahoo.com

Abstract: In the context of EU accession, Romania has pledged to reduce cross-border crime and illegal immigration, safeguarding its citizens by issuing biometric passports. Thus, the Romanian Government approved on 24 June 2008 an Emergency Ordinance which provides that the Romanian National Printing Company will produce an exclusive basis, a series of documents, such as biometric passports. Conceptual architecture that describes the technical implementation of the ePass is related to two basic elements: the solution components and operational model for implementation. The components describe the entire hierarchy of components in accordance with the responsibilities they have static relationships between them and how they collaborate to deliver the functionality required of an IT system. Components are the primary concept used in a modular design. A component can be defined as an embedded part of a system that has a well-defined interface that is accessed through its services. Next we present the main components of this system architecture.

Key-Words: electronic passport, biometrics, architecture, concept, system.

1. Introduction

In the context of EU accession, Romania has pledged to reduce cross-border crime and illegal immigration, safeguarding its citizens by issuing biometric passports. Thus, the Romanian Government approved on 24 June 2008 an Emergency Ordinance which provides that the Romanian National Printing Company will produce an exclusive basis, a series of documents, such as biometric passports. Implementation of electronic passport personalization followed:
- increasing levels of automation, protection and accessibility of data,
- reducing the effort of moving people,
- increasing the efficiency of control and data exchange to reduce illegal migration,
- strengthening the fight against cross border crime

Strengthening security border of Romania.

This principle is that the data collection and issuing requests, respectively, by the person receiving the documents will take place decentralized in cities that are residence of persons, or accommodation centers, while customizing documents will be centralized.

Issuing system (ePass) complies with ICAO DOC 9303 [1], current edition and future ICAO biometric standardization, established in ICAO technical reports and specifications and all EU regulations. The biometric documents produced by Romanian National Printing and customized by National Center for Personalization of Electronic Passport are:
- Electronic passports to Romanian citizens,
- Electronic passports for stateless persons
- Electronic travel documents for the refugees
- Electronic travel documents for asylum in Romania
- Electronic diplomatic passports
- Electronic service passports

Legal authorities to record and release these documents are the Ministry of Interior and Administration for the first four types of documents and the Ministry of Foreign Affairs for the last two.

Main objectives were:
- introducing electronic travel documents;
- transfer of technology on production of passport blanks and sheets of
polycarbonate in the application of Government Emergency Ordinance No. 189/2002 regarding the offset operations related to procurement contracts for defense, public order and national security;

- establish a modern method of issuing electronic documents that will provide greater economy, efficiency and validity of this management process, and reduce the possibility of falsification of documents;
- defining and establishing a process to identify the person by biometric verification;
- creating a modern infrastructure by setting up offices for direct download individual data including facial image, signature and digital impressions.

In the description of the national system for issuing electronic passports Romanian will refer to a number of entities whose responsibilities within the system is well to mention:

1. Romanian National Printing Company is responsible for manufacturing the blank electronic passports and other similar documents, and related activities. The company owns the issuing system and has primary responsibility for maintenance and related support.

2. Ministry of Interior and Administration (MIA) is the legal authority to record data and release:
   - Electronic passports for Romanian citizens;
   - Electronic passports for stateless persons;
   - Electronic travel documents for refugees;
   - Electronic travel documents for asylum in Romania.

3. Ministry of Foreign Affairs (MFA) is the legal authority to record data and release electronic diplomatic passports and electronic service passports for Romanian citizens.

2. ePASS features

ePass provides the following workflow between its main levels:

<table>
<thead>
<tr>
<th>Activities</th>
<th>Request Level (RL)</th>
<th>Central Level (CL)</th>
<th>Manufacture Level (ML)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Offices of MIA and MFA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checking</td>
<td>Offices of MIA and MFA</td>
<td>MIA</td>
<td></td>
</tr>
<tr>
<td>Approval</td>
<td>Offices of MIA and MFA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customization</td>
<td>MIA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Final checking</td>
<td>MIA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sending</td>
<td>Offices of MFA</td>
<td>MFA</td>
<td>MIA</td>
</tr>
<tr>
<td>Release</td>
<td>Offices of MIA and MFA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.1. Application

The person requests the electronic passport and shows the necessary documents for requesting. The operator:

- shall verify the identity of the personal documents of identity or marital status;
- introduces the applicant's Numerical Code into the IT Application;
- checks the person's data in existing databases;
- places the other information required (date of payment, mode of release, etc.);
- sets out how the issue of passport
- prints the application and check the date with the applicant.

The person signs the application. The operator takes biometrics (photo and fingerprint) and electronic signature of the applicant the application then is saved in a national database

2.2. Checking

In the BackOffice employees of passport department:

- check the old files existing in the passport archive;
check in other databases available to the issuance approval stage;
scan documents accompanying the request of the applicant and saved in central database the electronic records of the person (at the first registration of a new application for issuing a electronic passport they will scan also the old files of applicant);
complement other data of interest to be stored electronically.

2.3. Approval

Based on previous checking, the worker:
- approves or not the issuance of biometric passports;
- takes the decision to cancel or not the previous passport, based on request of applicant.
At this level the data for customization are complete and available.

2.4. Customization

The data for customization are extracted from national database and local stored. At this level the passport blanks are customized.

**Final check** consists of:
- technical quality control of passports;
- checking accuracy of the chip data and of the polycarbonate page data;
- recording of passport number in the national database.

**Sending** consist of:
- create lots of passports for shipment to various destinations;
- preparation of passports in automatic (manual) for shipment by courier;
- delivery of passports.

**Release** consist of:
- checking person identity based on personal documents and records of databases available;
- recording a second signature of person in the national database, and visual comparison of existing signatures;
- the actual release of passport.

3. ePASS system parameters

To better understand the size ePass should we review some of its parameters:

- **Performance.** Achieving these performance criteria is the maximum system load conditions.
  - Read operations of simple database records do not last more than 4 seconds;
  - Write operations of new entries in the database does not last more than 4 seconds;
  - run any report from the list of reports (statements) current will be completed no later than 7 seconds.

- **Information Volume:**
  - The maximum number of passports issued national daily: 12000;
  - Average number of passports issued national daily: 5000;
  - The maximum number of passports issued in a calendar year: 1600000;
  - The average size of folders: 20MB;
  - The total size of county databases current system: 256GB.

- **Availability of server and communications:**
  - Operating range: 24 hours x 7;
  - Percentage of availability: 99.95% monthly;
  - The downtime allowed: 20 minutes per month.

- **E-mail Information Volume:**
  - Number of users (mailboxes): 5000;
  - Size of mailboxes on the server: 500 MB.

- **E-mail Availability**
  - Operating range: 24 hours x 7;
4. Conceptual architecture of ePASS system

ePass architecture that describes the technical implementation of the ePass is related to two basic elements: the solution components and operational model for implementation. The components describe the entire hierarchy of components in accordance with the responsibilities they have static relationships between them and how they collaborate to deliver the functionality required of an IT system. Components are the primary concept used in a modular design. A component can be defined as an embedded part of a system that has a well-defined interface that is accessed through its services. Next we present the main components of this system architecture.

4.1. Load-balancing Component

The load balancing node supports intelligent load balancing that directs user requests to the server that can serve them best. Specific features:
- Provides load balancing for all access point in the IT system;
- Ability to configure for High Availability
- Supports Web Services;
- Distribution of workload for Web servers;
- Provides routing of requests between HTTP, FTP and TCP-based servers.

4.2. Web Interface Component

The Web interface:
- allows use of the ePass using a web browser;
- is located in DMZ;
- performs the functions of authorization / authentication.

As a specific feature, it is with systems management and monitoring, logging and security solution. Web interface includes the following components:

Reverse Proxy Node

This node is a replacement for web server in the DMZ. Node receives requests to server applications to web applications and server applications. For issuer demand node appears as the web server. Reverse proxy server provides security services, redirection, access and traffic associated with the application. Also creates a barrier between the business logic of applications and external access points. Node works with the access management component and communicates with it through the firewall, using specific ports and protocols. Specific features:
- Network Address Translation - All internal addresses are hidden to end users who access internal applications
- Support for global authentication (SSO) - Reverse Proxy provides global authentication mechanisms that allow access to more resources or different applications without requiring user reauthentication if the new resource or application requires a higher level of authentication
- SSL Certificates Support Split - Reverse Proxy mechanism provides SSL server support for certificates of external systems.
- encryption mechanism - the product supports the following encryption mechanisms: 1:40-bit RC2 0.128-bit,
40-bit RC4, 128-bit RC4, Data Encryption Standard (DES), 56-bit DES, 168-bit triple DES security features;

- Link through proxy - All network connections to resources and applications in the DMZ or internal are initiated by the reverse proxy server. Network addresses or "namespaces" foreign customers are not allowed in the DMZ or internal Web servers or applications.

- Authentication methods - reverse proxy server supports the following authentication methods:
  - username / password;
  - X.509 client certificate;
  - token authentication;
  - NTLM authentication;
  - LDAP;

- Support for login authentication with two actors - reverse proxy server supports two-factor authentication tokens and hardware by combining two single-factor authentication methods such as X.509 certificates and username / password.

**Web Server Node**

This node provides a web server that delivers content and process the information mainly static nature. Static pages (and pseudo static) are delivered based on HTTP protocol. If the request is to access some dynamic content, than Web server forward requests to the applications server.

**4.3. Process Services Component**

These services are responsible for the implementation of process workflows. They include mechanisms for enforcement and management of business rules and processing field decisions.

Processes can be short, non-interruptible, or long-term, including combinations of services provided by software and human actions.

Component is associated with the following node:

**Process Node**

The software application is built around a workflow management engine that registers each stage of the process of issuing electronic passports (including the release of the temporary passport). The application also incorporates a module for document management and electronic archiving, which allows the electronic transfer of documents attached to the passport issuing form. Scanning activities is done using MFP printers.

ePass is designed as a flexible, able to adapt easily to changes in the law by using a rules engine that allows you to modify business rules without rewriting the application.

The process server allows the development and execution of business process flows of ePass and supports the implementation of business rules.

Specific features:

- Supports BPEL standard;
- Supports SOA architecture (Service Oriented Architecture);
- Support the implementation of short running processes and long running (that require user intervention):
  - allows transactional processes (commit / rollback) for the running short processes;
  - Offers compensation mechanisms for long running processes. For each step of execution, or execution sequence, the process offers the possibility to define a compensatory action opposite.

- Process Server provides error handling mechanisms;
- Supports the integration of user actions as steps for implementing the process
- Allows user management role-based;
- Process Server provides the ability to define and manage business rules in a tool for personnel without technical tasks;
- In addition to processes based on BPEL (Business Process Execution Language) Process server supports event-oriented process based on the concept of UML state diagrams.

**4.4. Applications Component**
Application component implements the business logic of ePass. The ePass system includes business application components at two levels:
- Components for capturing, modeling the applicant and the registration of personal data and biometric collection
- Management components that are responsible for the centralized storage of personal data and folders of documents. All these are subject to validation, checks internal data sources or external system, while being subject to an approval workflow; these documents managed within this workflow are archived based on online data retention policies;
- For checking, application components communicate with public records databases from county and central level.

Business application components are integrated in a unified vision of the controlled engine that manages workflow processes and business rules. Node application component includes:

**Application Server Node**
Application server has the following features:
- Ability to integrate with other system components, or its future extensions based on open standards
- Clustering capabilities with intelligent workload distribution in the cluster
- Distribution of web server workload
- Can provide web services using SOAP protocols, HTTP, JMS
- Integration with the Web server node
- High availability and backup for transactions
- Support for role-based authentication and certificates
- Administration and monitoring components

### 4.5. Database Component

All data management application modules for electronic passports (including electronically stored documents) are stored in central database, where it can be accessed by all users of the structures. Component provides data storage media and mechanisms to store these data. Data component is able to provide access control mechanisms, so that data cannot be accessed by avoiding unauthorized access mechanisms from the application server.

**Database Node**

Specific features:
- To be able to store, query and return alphanumeric data;
- Stores multimedia data and biometric records attached alphanumeric;
- supports Unicode UTF-8;
- Supports communication with client applications using the transport protocol TCP / IP;
- supports systems such as Windows, Unix, Linux;
- Provides reporting functions and integrate easily with external reporting tools.

Security features:
- allows you to restrict access to the database objects;
- allows implementation of multiple security policies on the same database object;
- provides a list of operations that a group or class of users can execute;
- offers a feature that records the following information changes, insertions, deletions and selection by individual users, internal object database:
  - a user ID database (ID as it is stored in the database);
  - a date and time (date and time of action);
  - a transaction type (select, insert, modify, or delete);
  - an ID database;
  - a subject / target objects;
  - query sent;
- provides a mechanism for verification and validation of passwords;
- provides a mechanism for data encryption.

Backup and restore features that are provided:
- a facility for total saving or partial saving of database;
- provides a facility for total restoration or part restoration of the database;
- a facility to record all database changes to allow recovery of the database;
- a facility for full recovery or part recovery of the database at a user specified time;
- the ability to make backups for one or more table spaces allocated as specified by the database administrator;
- saves online database directly to tape;
- a database restore directly from tape;
- write more files on the disc simultaneously during a rescue operation;
- read from disk files simultaneously during a restore operation;
- parallel reading and writing during a rescue operation;
- enables high availability architecture.

4.6. Integration Component

Component integration architecture implements a bus service in the ePass. This bus provides infrastructure to integrate distributed, able to operate in a heterogeneous environment. Component includes a series of nodes detailed below.

Integration Node
Integration node provides a "front end" to systems running legacy applications on nodes. Node provides secure points of access using different protocols of legacy applications through the use of a catalog of internal services and implementing a service-oriented architecture.

Features of interaction, transformation:
- connectivity between any points;
- intelligent routing capabilities based on routing rules;
- Convert transport protocols;
- Changes to format messages in real time;
- Support interactions using JMS, SOAP / HTTP (s);
- Support for Web services standards and technologies and traditional protocols;
- Support for processing incoming files via FTP;
- Ensure the integrity of transactions and interactions;
- Supports and manages interactions between services;
- Supports different styles of interaction: messaging, request/ reply, publish/subscribe and events
- Provides logging messages;
- Ability to convert syntactic;
- semantic transformation (mapping) between different formats and data structures;
- Conversion of data fields that are transferred between database schemas defined;
- It can handle input and output data defined in different encoding and character set;
- Supports both Unicode and associated conversions and for more data encoding and languages for data storage;
- Ability to import standard data structures such as XML, CSV, and database schemes other standard schemes;
- Ability to use databases for features of "lookup" or complex data transformations. Access to database is made directly from the integration platform;
- Support for message queues as the main protocol for delivering messages;
- Support for TCP / IP and HTTP, FT;
- Support for JMS protocol for both reception and transmission of data
- Support for different transport standard protocols for receiving and sending messages;
- Ability to save expired messages or those processed with error reporting for analysis later;
- Provides targeting messages based on events;
- Ability to process correctly a set of messages to be transferred to a strictly specific;
It can trigger a certain process, based on a set of events;

- Ability to perform a transfer of transactional information, the ability to define transactions over the platform integration and JMS providers;
- The ability to route messages in parallel;
- Ensures delivery destination of messages, and deliver a message only once;
- Provides support for authentication and encryption at the transport level;
- Provides generation of reports on the different stages of message delivery (delivery to application timeout, error, etc.);
- Support for version control, including the ability to rollback;
- Connectivity based on open standards;
- Java APIs, C++, .NET and others in order to develop custom modules to connect;
- Possibility of use of existing connectors to connect to applications based on technologies: JDBC, TCP/IP, HTTP, COM, EJB and others.

**Folders of Web Services Node**

Service registry is a component that allows storing and managing metadata about services implemented within the solution.

Register of services offers the following features:

- Provides the ability to manage the entire lifecycle of a service: from definition phase to the exploitation of the production environments;
- Allows identification of services so that they can avoid duplication of services;
- Enables Interoperability with Enterprise Service Bus type systems and any other platform that exposes services or performing mediation services;
- Supports interoperability between services, through support for the following open standards: Web Services Description Language (WSDL) \[2\], XML, XML Schema Definition (XSD) Language, Business Process Execution Language (BPEL). \[3\].

**4.7. Security Component**

Application components designed and implemented benefit from advanced security features, which include:

- the application user management, role-organized, hierarchical;
- functionality of a particular user can be allocated only through a role;
- Keeping of detailed log files of all transactions made by users and administrators.

Security component involves several components:

**Components of authentication, authorization and identity management.**

The components of authentication, authorization and identity management accesses meet the following features:

- Identity Manager (IM) allows centralized users profiles management in the organization. A person can have multiple user accounts in different application systems, DBMS, application modules. Identity Manager manages associations between a people, a user account with appropriate access rights. Identity Manager maintains a database of all identities and access existing accounts in the organization. This database is stored in a server catalogs (catalog identities).

  When you create an identity, Identity Manager (IM) systems creates user accounts based application role that each person has in the system. It's also created a new user accesses the Manager (MA) for the user to be logged in web applications.

Manager accesses (MA) provides a policy-based security model. MA secures web environment, the flow of messages in the media integration applications or operating systems. This module provides facilities such as:

- User Authentication;
- Control access privileges;
- Auditing;
- Single sign-on;
- High availability;
- Logging.

MA components include:
Policy Server (PS): It manages the master authorization database for the secure. This server is key component to execute applications for access control, authentication and authorization. It stores all user profiles and accesses control lists;

Component Validation Access (CVA): The component is responsible for enforcing security policy. CVA check if a user with SP is allowed access to a protected resource, allowing access based on this check;

Administration Manager (MAD) provides a management interface. Proxy Server Policy (SPP) is a copy of the SP. In this case, is located in the DMZ to remove traffic from the DMZ to the management area between. CVA is running checks with SPP and not SP. SPP is regularly updated by the SP.

When a user wants to access a web application accessed through a browser component CVA verifies that the requested URL is protected and attempts to authenticate the user. CVA supports different types of authentication (basic, forms-based authentication based on SSL certificates based on chips, etc.). Once logged in, CVA transfer request HTTP server (or server applications) with user credentials. Application Server checks whether the user can be found in the catalog of users. If the user is found, then access is granted and the HTTP response is sent back to the browser.

Specific features of the components Manager Identity and Manager Hits:

- Provides the capability to detect any change in real-time information about a user (name, password, other property) that appears in any source that contains that information and propagate that change automatically to any other source that contains information about that user. Propagation mechanism is configurable:
  - User can retrieve information from multiple sources: unformatted files, XML files, databases, directory servers;
  - Is compatible with multiple sources that store identity information (such as HR systems, databases, files, directory servers);
- Provides the ability to assign or change user rights/privileges of access to the organization based on existing policies in the organization and the user’s role in the organization;
- Provides the ability to delegate responsibility to management departments or other units of the organization;
- Provides the capability to allow users to manage their passwords, including change and reset passwords without administrator intervention;
- Allows users to request the creation of new accounts using a web browser (user self service);
- Allows users to update their personal information and to disseminate the information automatically to all resources of the organization containing all or part of that information;
- Contains a workflow engine that directs any request to the approver; notification should be made through an email;
- Can simulate any changes to information about users, policies before the change;
- Provides the ability to view any user requests or requests concerning information about changing user demands;
- LDAP integration and application server - the solution contains an LDAP directory server to manage users and integrate with server applications;
- Policies and restrictions - solution enables configurable security policies which enforce access restrictions based on time, IP addresses to limit the access to resources. The solution enables these policies allow users to only those resources that have protected the right to access, depending on their role in the organization;
- Centralized management - provides centralized management
solution for managing users, groups, roles, permissions, policies. The components of authentication, authorization, identity management will be integrated into the node architecture:

**Security and Components Catalog Node**

This node is a collection of components catalog along with the data necessary to implement a structure of catalogs in the entire organization. Node is implemented as a single server catalogs. Components Catalog maintains information about the characteristics of resources such as network name or address and date of creation.

Business logic processes characteristic of node support components catalog:
- Management of catalogs: the catalog entries and update management;
- Catalog Search Engine: A search facility and access to content catalog;
- general applications on catalogs: business applications that report content catalogs.

Business logic associated with data stored in the node to authenticate and authorize users to access e-business applications and services

Catalogs and security node states:
- Security services (a subset);
- Authentication Required information;
- Access Rules;
- Services to the organization (subset).

There are implemented border servers to protect the internal network traffic against unauthorized transactions. Servers border nodes within the solution include detailed below:

**Protocol Firewall Node**

Protocol firewall node has the role of point of entry into the demilitarized zone (DMZ). Public firewall node filters and manages data flows in the DMZ of WAN ePass. Typically this role is performed by a router firewall. The basic concept is that only certain protocols are allowed passage through the firewall (eg HTTP on port 80). A firewall router is different from normal IP router in that it applies a set of technologies for IP packet analysis to decide whether a package is allowed passage through the firewall or not. A firewall is also called filter screening or packet filter. Additional facilities selective filtering node also provides logging and reporting capabilities for the types of traffic flowing through the node. Node can also use different technologies or alteration of information in the encapsulation of IP packets (eg tunneling).

Node provides IP filtering, audit logs, to facilitate tracking and monitoring.

**Domain Firewall Node**

Domain firewall node controls access to internal network organization within the DMZ. Similar to the protocol firewall, the firewall examines traffic passing through it, blocking any information that is not explicitly allowed in the internal rules of the node. The domain firewall will only allow requests from the DMZ to the node node (or nodes) of the application and appropriate responses to these requests.

Firewall devices demarcation following security zones:
- Management Area;
- Development Zone;
- Manufacture area.

**Organization Firewall Node**

Firewall secures an organization's internal network organization ePass networks by allowing more specific protocols such as Java Database Connectivity (JDBC) or the Message Queue Interface (MQI).

Firewall devices demarcation following security zones:
- Management Area
- Development Zone
- Manufacture area

Manufacture area is bounded in a DMZ that includes integrations with external systems and internal applications and available data.

**4.8. Logging Component**

Adopted solution allows the organization automate log collection, implementing an alert system and get a platform to increase security investigation and avoid
exposure of sensitive data at risk. The solution is in compliance with security rules by a secure log collection and storage, reporting and alerting events from heterogeneous systems. Specific features:

- Collect log in securely;
- Provides a flexible online storage that can store as many logs as much time;
- Reporting Intelligence solution provides predefined reports and can create new reports. These reports are distributed and exported into popular formats: pdf, excel, text, csv;
- Improve security and performance
- Provides a specialized module for File Access.
- audit activity and changes in Active Directory showing the following features:
  - offers support for compliance;
  - offers full automation;
  - a monitor user activity;
  - guarantees the integrity of a log;
  - data compression anomaly analysis;
  - generates alerts in real time;
  - generates flexible reports;
  - easy to use management reporting interface.

The component management system uses this node.

4.9. Management and Monitoring Component

The monitoring and management component serves ePass components and ensure their consistent level of service policy of the system.

ePass management component aims at monitoring the implementation of three applications and a service desk application with the following features:

- monitoring network status;
- monitoring systems and applications;
- client management and software distribution;
- Service Desk;
- monitoring smartcard.

Such monitoring is implemented by the operational center of the network and data center servers and automate customer management (inventory, software distribution).

Component management system uses:

**Node management**

Node represents a collection of system administration and system management processes needed to implement a data management system centralized systems. This node acts as an initiator and central collection point for all system management tasks (ie collecting polling alerts the equipment etc).

5. Conclusions

Now all this architecture described above is working.

With the implementation of this infrastructure, Romania have for the first time a centralized IT & C system to issue passports and was the first European country who implement simultaneously in the electronic passport both facial image and fingerprint.

References

(The author of present article was part of team in charge with specifications development)