Signature WEB

Application
for the Management
of authorized Signatures

A comprehensive solution that allows banks and financial organizations to organize, maintain and distribute over the WEB the List of bank's authorized signatures

out sourcing
B&R outsourcing services SA

The business

Nearly 50 million lists of authorized signatures are exchanged between banks - partners worldwide each year, an unnecessarily large number, as only a few signatures are required. Most banks also distribute these lists internally further increasing the number of copies. The disadvantage of this schema includes high production costs, long delays in retrieval of signatures and, most important, lists that are not up to date. Many banks also want to have their authorized signatures stored in an internal host sharing their lists even with their subsidiaries.

The solution:

The traditional solution was to create Signature Books or CDs containing the samples and to physically transport sensitive material by mail or deliver them by hand. This solution was slow, inconvenient, insecure and prone to errors.

SignatureWeb application offers a comprehensive solution that allows banks and other organizations that have similar problems, to organize and maintain the list of authorized signatures of their executives. On the other hand it allows authorized users to have immediate and up-to-date access to the managed signatures to obtain visual samples for authentication purposes.

The application interface is intuitive and user friendly, while it provides complete security during storage, transferring or managing data. The hardware requirements of the application are minimal and the application is lightweight and cost efficient.

BASIC CHARACTERISTICS

- ✓ **Simple**: SignatureWeb is a low cost product that uses intuitive web interface and has an extremely short learning time.
- ✓ **Secure**: Designed to rigorously deal with Security and Authorization issues concerning both user accounts and data. In addition, it logs all user accesses and keeps the history of data changes for auditing purposes.
- ✓ **Flexible**: It can be installed in whatever environment is available (any application server, any database supporting SQL, any operating system).
- ✓ **Convenient**: Designed in two components – a search utility (**SignView**) and a management module (**SignManage**) – that can work (and acquired) independently, allowing companies that already have management modules to import their data and make them available for searching to Intranet or Internet.
- ✓ **Smart**: Uses a compressing algorithm to minimize space requirements and enhance transfer speeds.
- ✓ **Universal**: Supports many languages (currently supports Greek, English, French, German, Spanish, Italian and Russian)

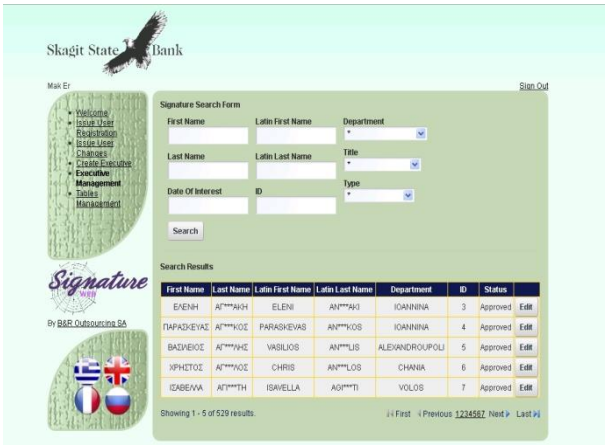
SignView The module allows users to connect to the server and search for sample signatures of Bank Managers.

- User access can be limited.
- Module Administrators can create accounts, define allowed functions and restrictions
- Several criteria (fields) can be chosen during installation.
- Partial fields can be used. If more than one field is used, result must match both criteria (AND).
- Multiple search results populate a list.
- Clicking any row of this list displays a pop-up window containing sample of the Manager's signature.
- The Manager's data are displayed on screen.
- Signatures cannot be clicked or downloaded.

SignManage The module allows the system administrators to manage the server database that contains data and signatures. "Four-eye" principle fully implemented:

✓ two administrator types (roles), Maker and Checker.

- Makers handle changes to database,
- Checkers handle updates and grant roles to users. Can access logs and history of changes.



- Define User restrictions.
- Import data (CSV) to records in the database.
- Obtain Signature samples.
- Add / Edit records in the database tables.
- Specify the validity period for every signature.
- Mark records that have exceeded the validity period as active or inactive.
- Examine log files and history of changes.

Advantages

- Allows Banks to maintain exclusive control over their own signatures, but can allow other users to obtain samples of authorized signatures for verification purposes.
- Increases the speed of obtaining samples
- Provides the ability to get samples any time of the day even on holidays.
- Increases the reliability of search results since the changes in the database are reflected in real time.
- Completely eliminates errors caused by transportation of physical objects like paper copies and CDs.
- Provides the ability to Import data and pictures using CSV files.
- Allows customers to easily migrate their data even from legacy systems.

Modularity in terms of:

✓ Content Management capabilities, separating content management from presentation style and layout management

✓ Implementing the MVC architecture, separating presentation from business logic and database access (using java technologies such as java faces, java struts, etc.)

✓ Deployment and component reusability, with the use of portlets technology, a java servlet-like software technology.

A transparent layer over the underlying DBMS:

✓ Program interaction with the database can be built on higher level technologies like Hibernate, which run in application server persistent containers, allowing the application server to manage both the transactional operations with the specific underlying DBMS and also the security of connection.

Implementation

SignatureWeb is built on top of the Liferay platform, which is a tool based on java technology for creating enterprise-level web portals. Liferay was chosen because it runs on any application server, database and operating system, so it eliminates new spending on infrastructure.

The use of an application server implies:

- ✓ Modularity in terms of:

  Content Management capabilities, separating content management from presentation style and layout management

  Implementing the MVC architecture, separating presentation from business logic and database access (using java technologies such as java faces, java struts, etc.)

  Deployment and component reusability, with the use of portlets technology, a java servlet-like technology of software running on the server side.

- ✓ A transparent layer over the underlying DBMS:

  Program interaction with the database can be built on higher level technologies like Hibernate, which run in application server persistent containers, allowing the application server to manage both the transactional operations with the specific underlying DBMS and also the security of connection.

B&R outsourcing services SA
39 Akadimias Street
GR 106 72
Athens, Greece
Tel.: +30 210 3208565
Fax: +30 210 3616536
http://www.outsourcing.com.gr
sales@outsourcing.com.gr

Security

Due to the inherent nature of the application scope as well as the intended users, SignatureWeb had to be designed to rigorously deal with Security and Authorization issues concerning both users and data. In addition to the inherent capabilities of Liferay, custom software had to be designed and deployed.

User access authorization: The system allows only authorized users to log in and access its portlets which expose the program's functionality, controlled by the Liferay user-management.

User access scope: Users with valid accounts have predefined limitations on the information they can access, controlled by SignatureWeb management system.

Data management authorization: SignatureWeb implements the "Four-Eyes-Principle". Changes on system data cannot be finalized until two administrators act, the Maker and the Checker. Only Makers have the ability to alter users or data, but no change has effect until a Checker approves the action.

Data management security: The managing module of SignatureWeb (SignManage) is implemented independently of the viewing module (SignView). This allows hosting the two modules on different domains, allowing SignView to be accessible from the internet and SignManage only from the intranet. This can significantly reduce the possibility of Brute Force Attacks on the Administrative part of the system, since potential attackers have also to bypass the underlying intranet security.

Sensitive Data security: Signatures are stored in a database, compressed by a proprietary algorithm and encrypted by the database. Thus it can only be displayed by the application, discouraging malicious users to browse through the images or otherwise use the information.

Data Transmission Security: The System to database connection is handled by the application server, using its inherent security. Transmission of Data over the Web can be achieved by hosting the application in a domain verified by a Certificate Authority (like VeriSign) and using SSL over http.