Identity Server (IDM) solution delivery reference

for the client ČSOB Stavební spořitelna – Building Savings Bank

(ex Českomoravská stavební spořitelna – ČMSS, a subsidiary of ČSOB bank/KBC Group)

The subject of the solution delivery is a system for user authentication and authorization compared to the repository of user identities in the form of Identity Server (IDM Server), providing at the same time:

- single sign-on (SSO) functionality
- multifactor verification
- audit log
- user and administrator interface
- a set of web services making available functionality as Identity Server
- operator training and follow-up support

INITIAL CONDITION

- **The client did not support single sign-on or multifactor authentication functionality for sales representatives or clients.**
- **Client authentication functionality was delegated to ESB services and subsequent application session.**

DESCRIPTION OF THE IMPLEMENTED SOLUTION

- Identity Server implemented the functionality necessary for further development of the multi-channel infrastructure of the ČSOB Stavební spořitelna client. It provides a secure, modern and standardized interface for single sign-on and authorization.
- ČSOB Stavební spořitelna enables potential clients to secure access to the self-service zone during self-registration or when logging in via social networks.
- For existing clients, it reduces the risk of misuse of access data to internet banking using the second factor (in the form of SMS + alternatively and using other verification methods), provides technical tools for possible modifications of the contractual relationship electronically (after verification by the second factor – SMS) and at the same time, it improves user comfort by unified login (SSO) to integrated ČSOB Stavební spořitelna applications.
- Identity Server also gave sales representatives more efficient use of integrated single sign-on (SSO) systems and significantly reduced the risk of unauthorized access to client data by the second factor (SMS).
- At the same time, Identity Server provides administrators an audit log with a detailed second factor of verified transactions in case of a future dispute.
- Identity Server is tightly integrated with other components of the multi-channel infrastructure, such as Liferay Portal, Client Identity Storage (LDAP), Web Services Front-End Bus (MCSB), the layout model and, in the future, the API gateway for access control (EC Directive – PSD2).

GEM SYSTEM

ČSOB Stavební spořitelna

Our solutions will satisfy you.

IDENTITY SERVER SOLUTION DEFINITIONS AND REQUIREMENTS

Identity Server provides authentication and authorization services to secure access for web and mobile applications to client services. The OAuth 2.0 protocol, wrapped in the OpenID Connect layer, was chosen as the security protocol.

IDENTITY SERVER PROVIDES THE FOLLOWING BASIC SERVICES:

- The IS authenticates the user's access to the New eLiška (NeL) application, the Mojeliška client zone (KZ) and for integrated applications accessing the MCSB directly.
- The IS issues and verifies the validity of the Access and token ID for request authorization and issues Refresh token.
- The IS provides the functionality of verifying the second factor via one-time passwords (OTP) sent in the form of an SMS to the user's registered mobile phone.
- IS provides web services (WS) and basic stylistic graphical user interface (GUI) for login and logout with redirection, user administration and self-service claims management. The user verifies the changes by the second factor.
- The IS provides an administration audit interface (GUI and WS) for authorized OTP transactions.
- The IS issues and verifies OTP for the access of the client, sales representative and for the execution of an active transaction according to the settings and values of the claim.
- The IS sends OTP via SMS gateway.
- The IS supports the second factor verification method by using a client certificate and mobile application.
- IS supports visual styles for various client applications.
- The IS provides an API for configuration and evaluation application permissions based on user roles.
- IS provides support for the use of password policies according to group policies in LDAP.

NUMBER OF USERS FOR THE LICENSE MODEL

- **Sales Representatives – Units of thousands of sales representatives**
- **Clients – 1–3 million clients**
- **Potential clients – about 10 million clients**

GEM System | Štětkova 1638/18, 140 00 Praha 4 – Nusle, Czech Republic | sales@gemsystem.cz | www.gemsystem.cz