# Introduction

## Review of the TMS/X functionality

The TMS/X application is used in order to prepare and send cash operations to the RTGS and ACH for processing.

The TMS/X also allows users to monitor:

* processing of transactions and requests, have been sent to the Central node,
* reports on transactions and message exchange;
* other information, related to the bank operations.

## Workstation requirements and settings

### Workstation requirements

Before starting to work with the Web interface system, make sure that your computer has been installed Microsoft Internet Explorer 10.0 or higher. The Java script should be enabled in web-browser settings. A client PC should have at least 512 MB of RAM and at least 1 GB free space on a hard drive.

### Browser proxy-server settings

If you operate via a proxy-server, find out its address and the port number from your system administrator. Set the received information in the correspondent fields of the IE “Tools” - “Internet Options” window ("Connection" – "LAN Settings" – "Proxy server"). If the proxy server will not be used, then no additional settings are required.

### ActiveX component installing and setting

No special installation procedures are required at the participant’s site, but **when a user connects to the system the first time, the user should allow installing ActiveX component** (in case user is going to sign and send transactions via TMS/X GUI manually). Web interface workplace is built on thin technologies and uses the standard browser for viewing its GUI.

To run genuine Windows validation, you have to install an ActiveX control. The Internet Explorer might not be configured to download ActiveX controls for security reasons, or you might have declined to install the ActiveX control when the Internet Explorer prompted you to download, install, or run the control. Do the following actions:

* Open the Internet Explorer;
* Click the **Tools** menu, and then click the **Internet Options**;
* On the ‘Security’ tab (trusted sites), click the Custom level button;
* Scroll down the Security Settings list until you see the ‘ActiveX controls and plug-ins’;
* For Automatic prompting for the ActiveX controls, click Enable;
* Scroll down to the ‘Download signed ActiveX controls’ and click Enable or Prompt;
* Scroll down to the ‘Run ActiveX controls and plug-ins’ and click the Enable or Prompt;
* Scroll down to the ‘Script ActiveX controls, marked safe for scripting’ and click the Enable or Prompt;
* Click the OK button and then click the OK again. (You may need to restart your computer.).

### Adding to Trusted Sites

Add the URL [https://<server>:<port>/portal/](https://localhost:8743/portal/) to trusted sites, where:

* <port> - TCP port for SSL connection to the TMS/X;
* <server> - name or ip address of the TMS/X server.

To do this, follow the steps:

* In the Internet Explorer, click **Tools > Internet Options**, and then click the ‘Security’ tab;
* In the ’Select a Web content’ zone s box, click **Trusted Sites** > **Sites** to specify its current security setting;
* In the ‘Add this Web site to the zone’ box, type the URL of the TMS/X site, and then click the Add button

Click the OK button two times to accept the changes and return to the Internet Explorer.

### Using only TLS 1.1 and TLS 1.2

In case you have to only use the TLS 1.1 and TLS 1.2, make the following setting:

* Left-click the gear icon;
* Select “Internet options” from the dropdown menu;
* Click the “Advanced” tab, scroll down and deselect “SSL 2.0” “SSL 3.0” and “TLS 1.0”;
* Select “TLS 1.1” and “TLS 1.2”;
* Click the OK button to accept your changes (it should take effect immediately, but you may need to refresh your browser).

### Disable compatibility view

In case you are using the IE 11version:

* Press the ‘Alt’ key on your keyboard, this will make a menu bar appear;
* Click on the **Tools** menu tab;
* Select the **Compatibility View settings** option;
* Uncheck the "Display intranet sites in Compatibility View" option.

## Starting the TMS/X application

The workplace is accessible via a standard link in a web-browser address line (the URL-address depends on the system’s configuration and shall be issued by the system administrator):

**http://<hostname>:<port>/portal**

where:

* <hostname> - a name or IP address of the host, where the web server is installed;
* <port> is a port number.

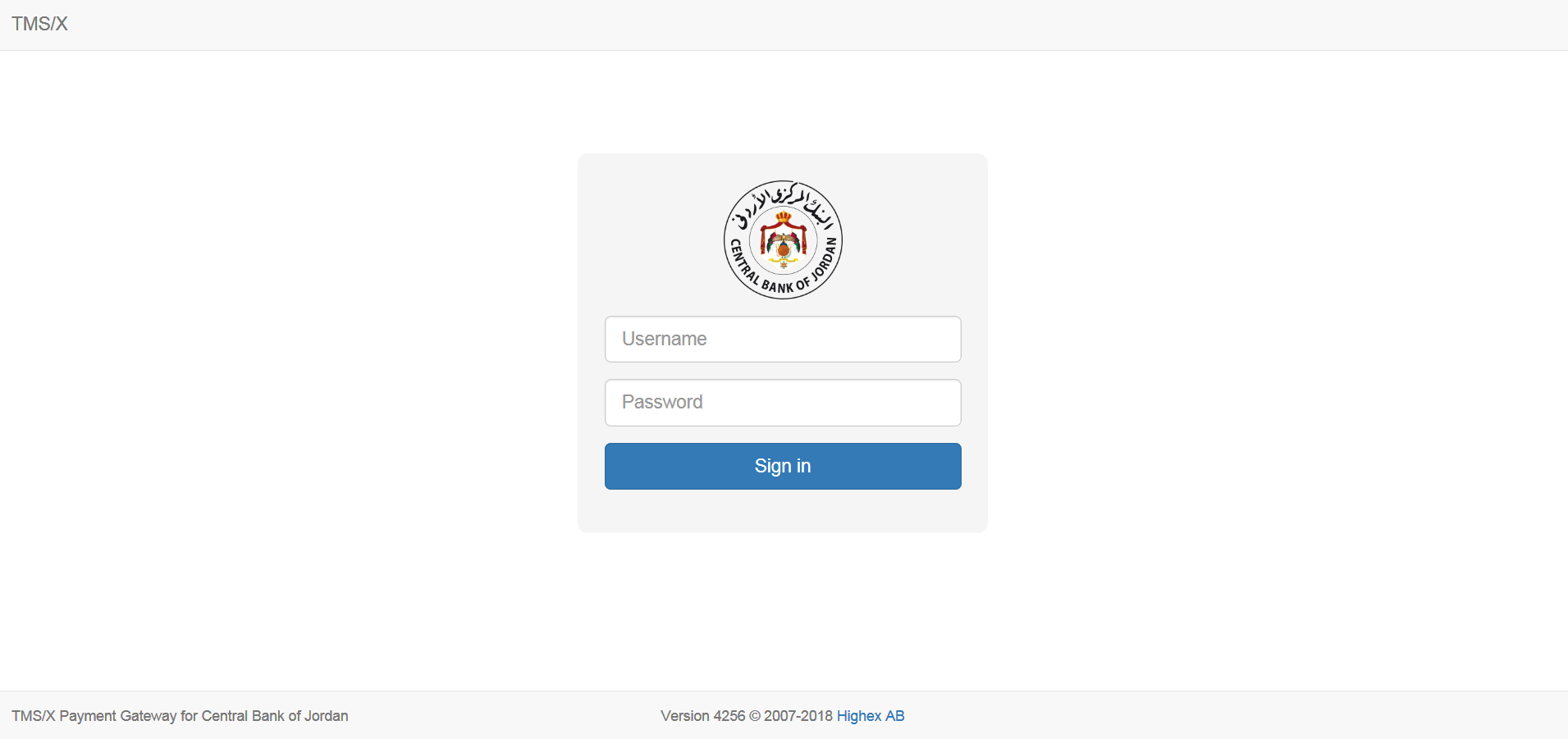
Example 1: <https://prism-client:8080/portal>

Example 2: <https://10.1.28.164:8080/portal>

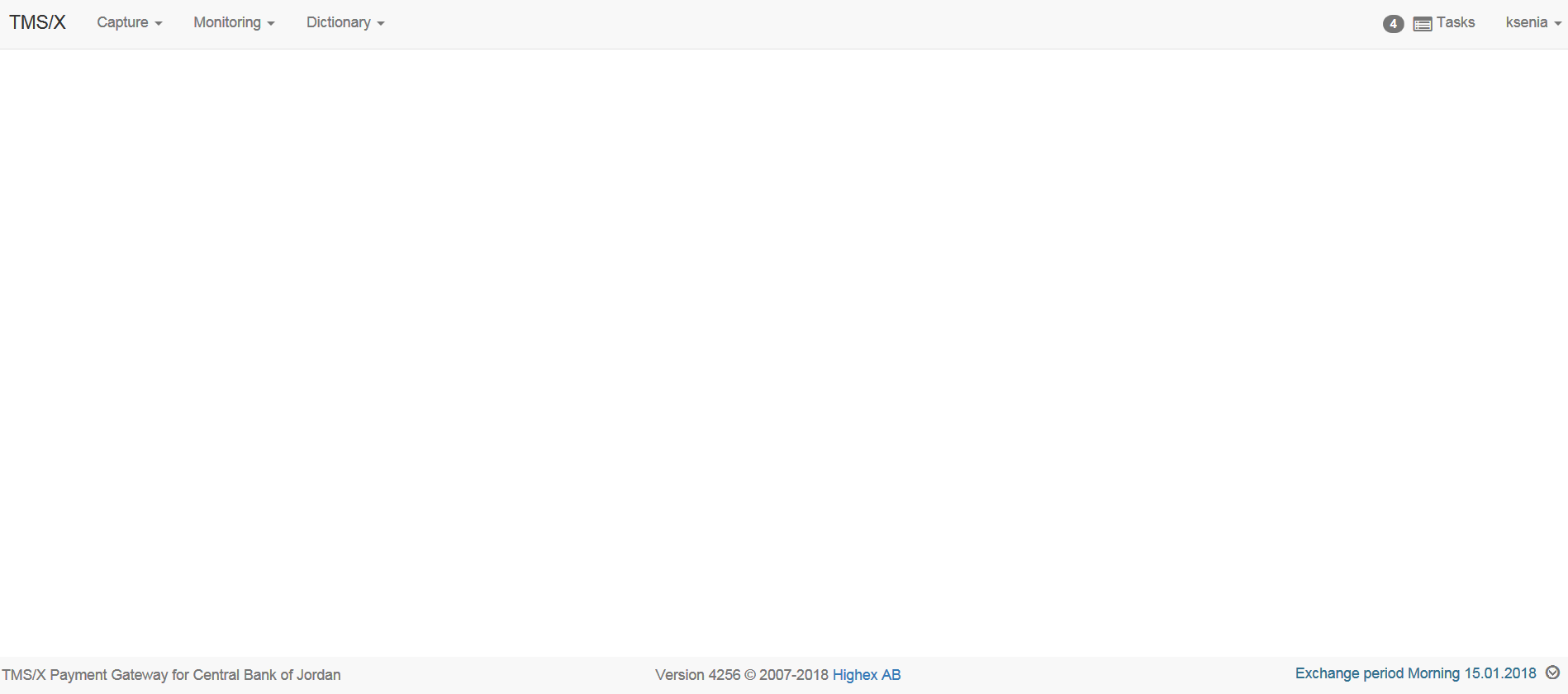
In order to launch the TMS/X application, call up the Microsoft Internet Explorer, specify the URL-address of the program and then click the "Enter" key:



A login form will be displayed:

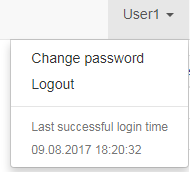


Each user shall be assigned a unique login and password for a registration on the TMS/X server (this is provided by the system administrator). Fill in fields of the form by your credentials and press the Sign in button. After the entered data was successfully verified, the user will get access to available options of the system, according to his(her) role, and the starting page will be opened:



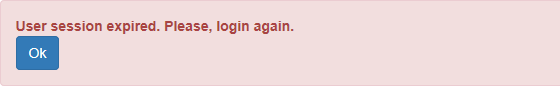
### Connect to the TMS/X

In order to close a communication session for the current user, click the username in the header of the TMS/X window and choose the ‘Logout’ command from the drop down menu:



A login form will pop up again, where you can enter another user’s login and password (e.g., to make authorization actions that were unavailable for the previously connected user).

The TMS/X server may interrupt current user connection due to some situations (e.g., in the case of long period of yours inactivity). In such cases, the TMS/X page will be blanked and the alert will pop up:



Try to login once more and in the case of a failure, contact to the system administrator or supporting team.

## User Role Hierarchy and Allocation

The TMS/X Workplace supports the following allocation of the user roles (each role defines set of access rights (permissions) to monitoring data and making operations):

* System Administrator – gives the permission to dictionaries, authorization profiles and switchover management;
* Security administrator – gives the permission to create user access and authorities’ management tasks;
* Security officer – gives the permission to approve user access and authorities’ management tasks;
* Operator – gives the permission create, edit and make transactions and transaction requests;
* Controller – gives the permission to authorize transaction and transaction requests.

The TMS/X administrator may assign one or several roles from the list to any user.

Each of the TMS/X users connects to the TMS/X by using his own login and password. After the user is connected, the TMS/X identifies the user’s role(s), which are definitely associated with the user credentials in the system. The contents of the TMS/X pages and menus will correspond to the identified user role.

# 