Krajowy Depozyt Papierów Wartościowych S.A.
KDPW_CCP S.A.
4 Książęca Street
00-498 Warsaw, Poland

T 22 537 93 43 | 22 537 91 27
F 22 627 31 11
E kdpw@kdpw.pl | ccp@kdpw.pl
www.kdpw.pl | www.kdpwccp.pl

SCP/ZW/3/2022
CCP/ZW/233/2022

Warsaw, 25 March 2022

**To: KDPW Participants**
**KDPW_CCP Participants**
**EMIR TR Participants**
**ARM Participants**
**SFTR TR Participants**
**Interested Parties**

**Re.: Modifications to KDPW and KDPW_CCP IT systems with regard to security of access to services provided over the Internet**

Dear Madam or Sir,

As previously announced at the meeting on 8 November 2021 regarding planned modifications to the KDPW Group's IT solutions in the area of access to services, please find below details of the planned modifications in the area of:

- the ESDI/Web communication channel (adaptation to the latest browsers); and
- access to the service portal https://online.kdpw.pl (addition of a second authentication factor).

These modifications require no adaptation in your IT systems and focus primarily on user interfaces in the process of accessing services offered using the Internet.
It should be stressed that the purpose of the modifications is to ensure an appropriate level of security when accessing the KDPW Group systems and applications which you are currently using.

## 1. Modifications of ESDI/Web – adaptation to the latest browsers

As part of communication based on the exchange of XML messages, ESDI/Web provides a tool for transferring information using a low volume of messages in the U2A (user to application) model by means of a graphical user interface. Access to ESDI/Web is granted by means of SWI certificates issued by KDPW which are used to authenticate the person sending the message. SWI certificates are also currently used as signature in Internet Explorer, for which Microsoft is phasing out its support.

The modification of ESDI/Web developed by KDPW in order to eliminate Internet Explorer, and thus the signature function, will allow the use of ESDI/Web in the currently leading web browsers. The authentication function using an individual SWI certificate will remain active (the process of obtaining a certificate from KDPW will also remain unchanged). However, to support verification of the integrity of the message, currently executed by means of signature, a hash function will be generated for the file submitted for transmission. The hash will be generated using public cryptographic algorithms, ensuring independent verification of the integrity of the message by KDPW and the sender. However, the modifications will not affect the process of sending and receiving XML messages via ESDI/Web.

In addition, it will no longer be possible to establish new connections to ESDI/Web via REST API. All Participants wishing to exchange high-volume messages are recommended to use ESDK based on a high-performance and secure MQ infrastructure.

The planned modifications of ESDI/Web will require amendments to the SWI Agreements concluded with the participants and to the Rules of the Information Exchange System (SWI). Annexes to the SWI Agreements will be presented to you for signature in time allowing their processing and the entry into force of the amendments to the Agreements on the planned implementation date.

**Tests:** We expect to make the test environment available and start testing with your participation as of **1 June 2022**.
**Roll-out:** Live operation of the modified ESDI/Web is scheduled to commence in production on **1 July 2022**.

## 2. Modifications to the services portal https://online.kdpw.pl - addition of a second authentication factor

In order to improve security of access to the services of the KDPW Group, taking into consideration the results of the risk analysis conducted in accordance with the Guidelines of the Polish Financial Supervision Authority (KNF) concerning management of information technology and information and communication environment security of market infrastructure operators, we are planning to introduce a requirement for authentication of services made available using applications within the service portal https://online.kdpw.pl. As a result, after the implementation of the solution, any access to services in the portal will require authentication with two factors (MFA model: multifactor authentication).

Requiring an additional authentication factor will provide additional security to ensure that the person attempting to access the KDPW Group's application is who they say they are and has all the necessary attributes to confirm it. By default (at the moment), authentication is done by entering the access account password, which is a credential of what the user knows. To improve credibility, a second authentication factor will be added based on a credential of what the user has. As a result, during

authentication, the user will be required to prove that they have access to a trusted and assigned device.

The trusted device will be :

- A mobile application (KDPW Group Authenticator) installed on an Android or iOS mobile device. The application can be downloaded for free from authorised stores: Google Play (Android), App Store (iOS - Apple). Its use will only be permitted on phones with unchanged security features of the operating systems of the indicated manufacturers. In order to act as a second authentication factor, the mobile application should also be linked to an appropriate access account (user's digital identity), which can be done after installation by the user.

or

- A trusted web browser, used on a computer on a specific network and IP address, which the user designates as trusted when logging in (after confirmation using the mobile app). The use of a trusted browser for login (after it has been designated as trusted) will be verified automatically during the login process as an additional factor of authentication to the designated user account.

The list of devices assigned to a given access account and designated as trusted can be managed in the account management options using a dedicated application: https://identity.kdpw.pl. The application allows users to remove devices from the trusted list as well as to verify all authentication operations carried out with a given device. It should be noted that access to the application will also require multi-factor authentication.

**Materials:** Detailed materials, including a KDPW Group Authenticator user manual, are available on the KDPW website at: http://www.kdpw.pl/en/MFA/Pages/default.aspx

**Tests:** We expect to make the test environment available and start testing with your participation as of **1 April 2022**. The first stage of the tests will involve a test intermediate site within the test environment, where users can understand the specifics of the second authentication factor. During this time, the portal https://tst-online.kdpw.pl will not support access on the current terms. As of **16 May 2022**, the second authentication factor requirement will be extended to cover access to all services in the test environment.

**Roll-out:** The additional authentication factor is scheduled to go live in the production environment (https://online.kdpw.pl) and the education environment (https://edu-online.kdpw.pl) as of **12 September 2022**.

### 3. Modifications to the data portal https://data.kdpw.pl – new reports and API

As part of the development of the Data Portal, we are planning to extend the service of paid access to reference and statistical data of the KDPW Group provided by KDPW in order to include API functionality compliant with the OpenAPI standard. Access to data via API will be an additional option available within the subscription. It can be ordered when creating a new subscription and added to an active subscription. API data download will be possible for the range of data (packages) to which

the client has access within paid subscriptions. Details of API access and rules of its operation will be included in the updated Terms of Service.

We have published a tab in the Data Portal dedicated to developers https://data.kdpw.pl/developers, containing the specifications of the Open API standard which we intend to use to offer automated access to paid reference and statistical data. The API will provide eligible clients with the ability to retrieve standardised JSON or XML data structures using typical HTTP protocol commands. The structures are already used for exporting data selected for interactive access via a dedicated GUI, and after the implementation of the API they will also be used for A2A (application to application) connections.

KDPW is developing both the technological and substantive content of the Data Portal in order to create a service meeting the needs of capital market participants for reference and statistical data. Our long-term goal is to provide you with a comprehensive range of KDPW reference data to the extent enabling you to optimise processes and operations performed in your databases. Therefore, along with the introduction of the API, we are also planning to launch new reports:

- Operations settled in KDPW by market;
- Registration of securities by the Issue Agent;
- Cash and derivatives market instructions cleared by the KDPW_CCP;
- Admission of instruments to KDPW;
- Withdrawal of instruments from KDPW.

We will keep you informed of the allocation of reports to packages via the Data Portal.

**Tests:** The possibility to test API authentication and authorisation is already available in the test environment. API Methods (Endpoints) for querying and retrieving responses for the first seven paid reports are also available. API Methods for new reports will be available for testing in the first half of April.
**Roll-out:** The roll-out of the API and new reports in the production environment (https://data.kdpw.pl) is scheduled for **16 May 2022**.

Yours sincerely,

Sławomir Panasiuk
Vice-President of the Management Board

C/C:
Narodowy Bank Polski (National Bank of Poland)
Giełda Papierów Wartościowych w Warszawie S.A. (Warsaw Stock Exchange)
BondSpot S.A.
Izba Domów Maklerskich (Chamber of Brokerage Houses)
Rada Banków Depozytariuszy przy ZBP (Council of Depositary Banks to the Polish Bank Association)
Urząd Komisji Nadzoru Finansowego (Polish Financial Supervision Authority)