**OPCOM Reporting** 

## Instructions for accessing the Reporting System of RRM Opcom

Data: 17.09.2015

Version: v1

## Introduction

The information download is performed from the dedicated server, which address is:

https://reporting.opcom.ro

The access is made based on Digital Certificate, username and password.

The Digital Certificate must be installed in the system from which the downloading of the notifications is wanted (computer or laptop). In Chapter 1 the modality of the Certificate installation is described and Chapter 2 describes the effective connecting with username and password and the files downloading.

## **Chapter 1 – Digital Certificate Installation**

The Certificate for connecting to <u>https://reporting.opcom.ro/</u> is submitted by OPCOM via e-mail in archived format (zip). For a higher security, the Certificate is protected by a password. The password is submitted separately, with the Letter accompanying the Agreement signed by OPCOM SA.

For installing it is needed, firstly, the Certificate to be unachieved from the received archive. You will obtain a file with extension pfx.

Then, the following steps will be performed:

- Launch (double click) on the unarchived file (pfx)
- Automatically, the window "Certificate Import Wizard" opens and a click must be done on the button NEXT:



- In the following window the path towards the Certificate must be verified. Usually, this is automatically set. If it is not correct, a click must be done on button Browse and the path towards the Certificate to be imported shall be chosen. Click NEXT.

Ce	ertificate Import Wizard				
	File to Import				
	Specify the file you want to import.				
	File name:				
	F:\OPCITINT\OPCITINT.pfx Browse				
Note: More than one certificate can be stored in a single file in the following formats:					
	Personal Information Exchange - PKCS #12 (.PFX,.P12)				
	Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)				
	Microsoft Serialized Certificate Store (.SST)				
	Learn more about certificate file formats				
	< Back Next > Cancel				

Then, the password received for the Certificate is introduced and it shall be verified if the box "Include all extended properties" is checked. In order to ensure the best possible security it is recommended the box "Enable strong private key protection" to be also checked. Then click on NEXT.

Certificate Import Wizard
Password
To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark this key as exportable. This will allow you to back up or transport your
keys at a later time.
Include all extended properties.
Learn more about protecting private keys
< Back Next > Cancel

- In the following window "Place all certificate in the following store" is selected, then click "Browse".

Certificate Import Wizard					
Certificate Store Certificate stores are system areas where certificates are kept.					
Windows can automatically select a certificate store, or you can specify a location for the certificate.					
Automatically select the certificate store based on the type of certificate					
Place all certificates in the following store					
Certificate store: Browse					
Learn more about <u>certificate stores</u>					
< Back Next > Cancel					

- A new window opens, where the directory "Personal" must be selected and click OK.



- Click "Finish".

Certificate Import Wizard	2 3-2-	×			
Completing the Certificate Import Wizard The certificate will be imported after you click Finish.					
	Certificate Store Sele	cted by User Personal			
	Content	PFX			
	File Name	F:\OPCITINT\OPCITI			
	∢	111 <b>•</b>			
	< Ba	ick Finish Cancel			
L					

- Click "OK".

Importing a new	w private exchange key
	An application is creating a Protected item.
	CryptoAPI Private Key
	Security level set to Medium Set Security Level
	OK Cancel Details

- In the moment when on scree apperas the window:



it means that the Certificate is successfuly imported.

## **Chapter 2 – Connecting to Server and Files Downloading**

For connecting to the server, from the computer on which you installed the Certificate as per step 1, access: <u>https://reporting.opcom.ro</u>



You will be required to allow the permission for the installed Certificate to be used:

Windows Security	×				
Select a Certificate					
	OPCITINT Issue: OPCOM MARKETS Valid From: 17.09.2015 to 10.09.2040 Click here to view certificate prope				
	OK Cancel				

In the following window you must select "Grant permission", and if you opted for a higher security and checked "Enable strong private key protection" during the process of Certificate importing, you must introduce the password you set during that stage:

Request For Permission to Use a Key			
Grant or deny this application permission to use this key			
Key name: Application supplied name for the key <ul> <li>Grant permission</li> <li>Deny permission</li> </ul>			
Key protection password:			
View key details			

A login a window appears, in which you observe that the username is automatically filled-in based on the selected certificate.

(c) (c) (c) https://reporting.opcom.ro/ $P = a c$ (c) (c) OPCOM FTP v1.6.2	×	□ <mark>×</mark>
OPCOM WEB FTP Username: OPCITINT Password: Login Save login details		

On this screen you will introduce the access password also received in the Letter accompanying the Agreement signed by OPCOM SA.

After login, you have access to folders depending on the services you selected in order to be performed by OPCOM.