User Guide

BTS® HTTPS ACCESS: TWO FACTOR AUTHENTICATION

Issue 1.4 | 29TH APRIL 2021

BORSA ITALIANA

TABLE OF CONTENTS

Revision History

Date	Version	Description	Author
27/1/2016	0.1	First draft	Borsa Italiana
5/2/2016	0.5	Internal review	Borsa Italiana
5/2/2016	1.0	First published version	Borsa Italiana
13/5/2016	1.1	BTS® registered trademark update	Borsa Italiana
20/6/2019	1.2	Updated BTS® URLs	Borsa Italiana
12/3/2021	1.3	Removed references to LSEG	Borsa Italiana
12/4/2021	1.4	Euronext rebranding	Borsa Italiana

1. INTRODUCTION

1.1 Scope

The BTS® is a multi market client application that works as trading and market data front-end for equities and derivatives markets.

Both brokering and market maker functionalities are supported, as well as additional functions to help activity control, supervision and post trading activities.

Algorithmic trading capabilities are also provided to enforce sophisticated trading and quoting strategies.

Different markets are currently supported:

- Borsa Italiana Cash markets;
- Borsa Italiana Derivatives markets;
- ETLX.

This document provides detailed information about procedures related to the authentication process related to the access to BTS® services via https protocol.

This access method does not require a local deployment of a client, nor requires the setup of an expensive leased line to interconnect with BTS® server infrastructure.

Security features of this access method are enforced, in order to comply with strict Borsa Italiana security policies.

BTS® https configuration and BTS® operating instructions are not considered in this document: you can find further information under **http://www.borsaitaliana.it/borsaitaliana/gestione-mercati/bts-bittradingstation/bts.htm**.

2. GENERAL

BTS® clients can access the platform over the internet by previously subscribe via Borsa Italiana Clients Technology Service Team (referred to as CTS in the following) this access method; the subscription is confirmed by a welcome e-mail which provides further instructions for finalizing the procedure.

In order to make the access secure, users must authenticate themselves by submitting two codes:

- a passcode (token), which is either:
  - generated by a software application manufactured by a third party (Secure Envoy), which runs on the user's PC or on the user's mobile device (handset/tablet);
  - sent by text message (SMS) from the BTS® to a user-defined mobile phone
- a password which the user themselves selects.

Purpose of this document is to describe how users access the BTS®. The document is divided into three sections:

Section 3 describes user set up and first log on.

Users who employ a soft token must perform the following three steps:

- download and install the Secure Envoy soft token software / app to their PC / mobile device, and configure it so that it communicates with the BTS®
- enrol themselves by (1) authenticating on Secure Envoy web page via the soft token by submitting their UserID, initial password and initial pass code, and then (2) submitting further information. At this point the soft token will start to generate pass codes
- log on to BTS® for the first time, which involves submitting (1) their UserID, (2) the initial password and (3) the pass code generated by the soft token. Users are immediately obliged to change their password. On subsequent logons users shall submit the selected password.

A user who employs text messages performs very similar steps:

- enrol themselves by accessing the web page provided in the welcome mail where they submit UserID, initial password and initial passcode and provide the destination phone number. Once this is done, Secure Envoy starts sending passcodes by text message (SMS) to the handset provided.
- log on BTS® for the first time as a soft token user, except that the passcode is provided via text message.

Users are requested to complete all of these steps in one dedicated and uninterrupted session to avoid problems with timeouts.

Section 4 describes the procedure for temporary pass codes.

Section 5 describes the procedure for password changes.

Section 6 describes the procedure for moving soft tokens between PCs.

3. USER SET UP AND FIRST LOG ON

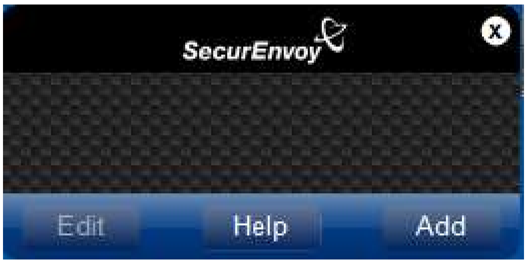
3.1 Download of the Secure Envoy Soft Token

3.1.1 Soft Token Users

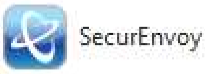
Instructions for the configuration process are in the document "PC Soft Token" attached in **Appendix A** and also available in the soft token zip file (see link in the next sentence).

Clients download the soft token software from **https://www.securenvoy.com/en-gb/support#id4**, install the soft token software and then configure the soft token software so that it points to the enrolment URL
https://secureauth.borsaitaliana.it/secenrol/
(**https://secureauth-cds.borsaitaliana.it/secenrol/** in test environment (CDS)).

Every single individual user must have a separate soft token – for example if a client has 9 users then there must be 9 soft tokens. A single instance of soft token software can support up to 6 soft tokens.



Once installed, the client will see that their Systray contains the following icon:



The client should then launch the soft token software and the box displayed on the left opens.

3.1.2 Text Message Users

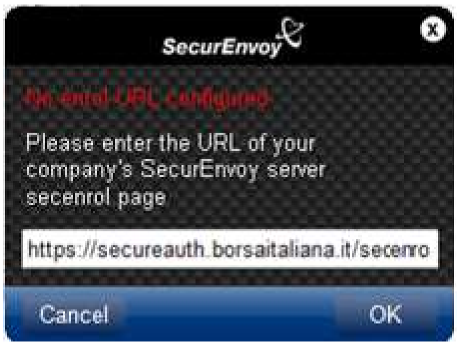
No step is required beyond providing the mobile number at enrolment time.

3.2 Enrolment

The user shall enrol only after receiving the **welcome email** an example of which is provided at the end of this section.

3.2.1 Soft Token Users

a) Select "Add", the popup reported on the right is displayed. The user enters the secenrol page URL **https://secureauth.borsaitaliana.it/secenrol/** (**https://secureauth-cds.borsaitaliana.it/secenrol/** in test environment (CDS)) and selects 'OK'.

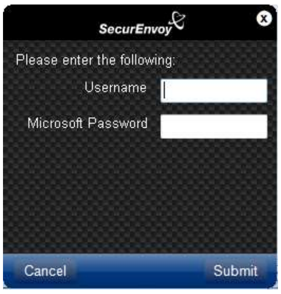


No enrol URL configured

Please enter the URL of your company's SecurEnvoy server secenrol page

https://secureauth.borsaitaliana.it/secenro

b) In the following popup the 'Username' shall be entered as provided in the **welcome mail** (see the text highlighted in yellow). This takes the form user.member. For example a username might be BTSUser0.9999**@bts.com**, where 9999 is the MemberID, BTSUser0 is the UserID and **@bts.com** is the BTS domain for production (@bts.test.com for CDS); in the field 'Microsoft Password' the BTS password shall be entered as provided by CTS. Select 'Submit'.

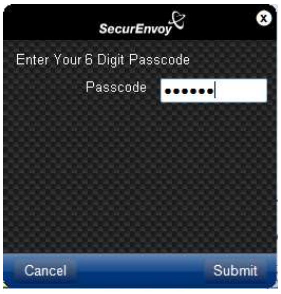


Please enter the following:

Username

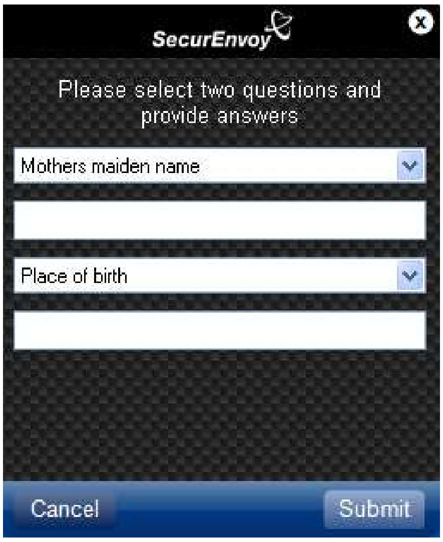
Microsoft Password

c) Enter the initial 6-digit Passcode notified to you in the welcome e-mail, which will have been sent by **no-reply-securenvoy@lseg.com** (**no-reply-securenvoy-test@lseg.com** for CDS)



Enter Your 6 Digit Passcode

Passcode ••••••



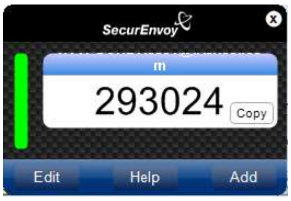
Please select two questions and provide answers

Mothers maiden name

Place of birth

d) The user will then be requested to select two additional security questions and specify answers so that they can access the self help facility (see **section 5**).

The enrolment process is now complete and the soft token will start to display pass codes, as displayed in the picture on the right.

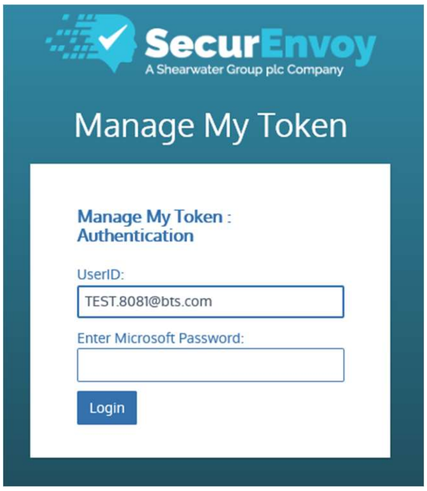


3.2.2 Mobile App Users

a) From the welcome mail select the enrolment site URL **https://secureauth.borsaitaliana.it/sechelpdesk** (**https://secureauth-cds.borsaitaliana.it/sechelpdesk** for test environment (CDS);

b) Enter in the page opened the UserID (in this case **TEST.8081@bts.com** or **TEST.8081@bts.test.com for CDS**, the field is pre-populated if the full URL is entered) and the BTS® password (field Enter Microsoft Password).

Select Login



Manage My Token

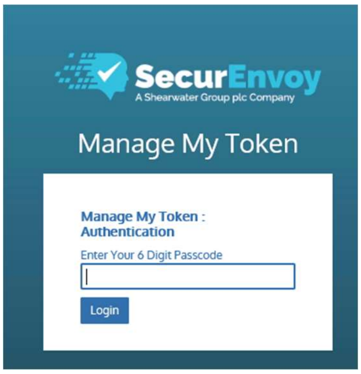
Manage My Token : Authentication

UserID:
TEST.8081@bts.com

Enter Microsoft Password:

Login

c) In the next page the passcode provided in the welcome mail shall be entered. Select Login.



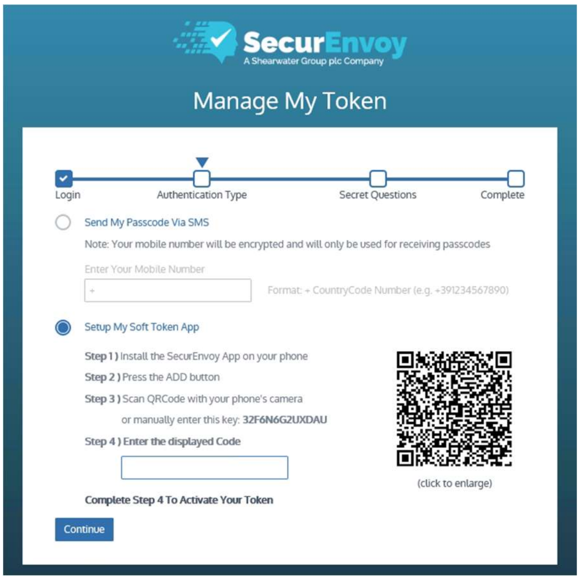
Manage My Token

Manage My Token : Authentication

Enter Your 6 Digit Passcode

Login

d) Users are now authenticated on the enrolment page, where they can complete the enrolment process. Select the 'Setup My Soft Token App' radio button and follow the instructions detailed in the page. It is necessary to have the SecurEnvoy app already installed and running on the handset while following the steps. Select Continue.



Manage My Token

○ Send My Passcode Via SMS

Note: Your mobile number will be encrypted and will only be used for receiving passcodes

Enter Your Mobile Number
+
Format: + CountryCode Number (e.g. +391234567890)

● Setup My Soft Token App

Step 1) Install the SecurEnvoy App on your phone

Step 2) Press the ADD button

Step 3) Scan QRCode with your phone's camera
or manually enter this key: **32F6N6G2UXDAU**

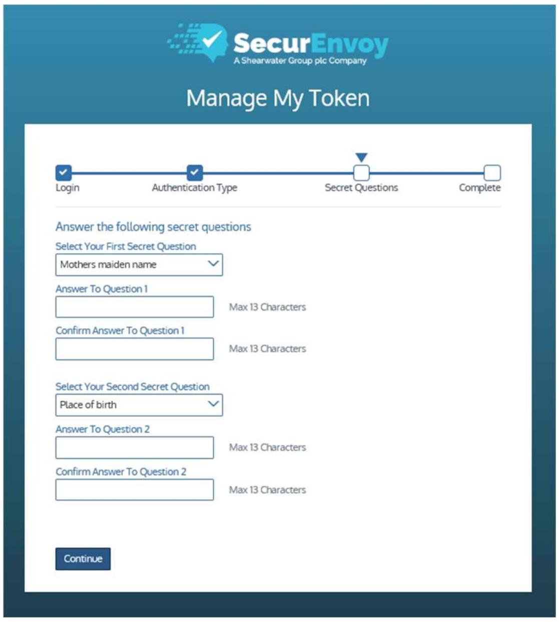
Step 4) Enter the displayed Code

(click to enlarge)

Complete Step 4 To Activate Your Token

Continue

e) Provide answers to the two secret questions, which shall be used when accessing the self help desk page. Select 'Continue' to close the process.



Manage My Token

Answer the following secret questions

Select Your First Secret Question
Mothers maiden name

Answer To Question 1
Max 13 Characters

Confirm Answer To Question 1
Max 13 Characters

Select Your Second Secret Question
Place of birth

Answer To Question 2
Max 13 Characters

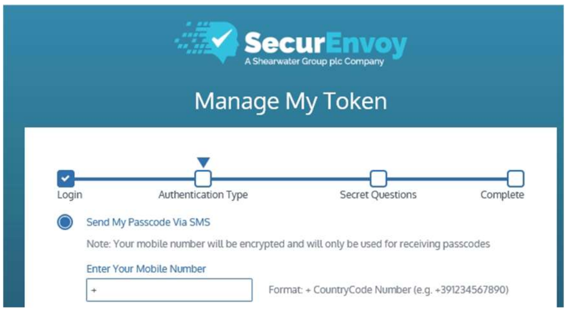
Confirm Answer To Question 2
Max 13 Characters

Continue

f) On the App confirm the name to be assigned to the token. Tokens are now displayed and updated automatically.

3.2.3 Text Message Users

The process is very similar to a Mobile App configuration, follow the steps described in the relevant chapter until b) included.



Manage My Token

● Send My Passcode Via SMS

Note: Your mobile number will be encrypted and will only be used for receiving passcodes

Enter Your Mobile Number: +

Format: + CountryCode Number (e.g. +391234567890)

a) Users are now authenticated on the enrolment page, where they can complete the enrolment process. Select the ‘Send My Passcode Via SMS’ radio button and follow the instructions detailed in the page.

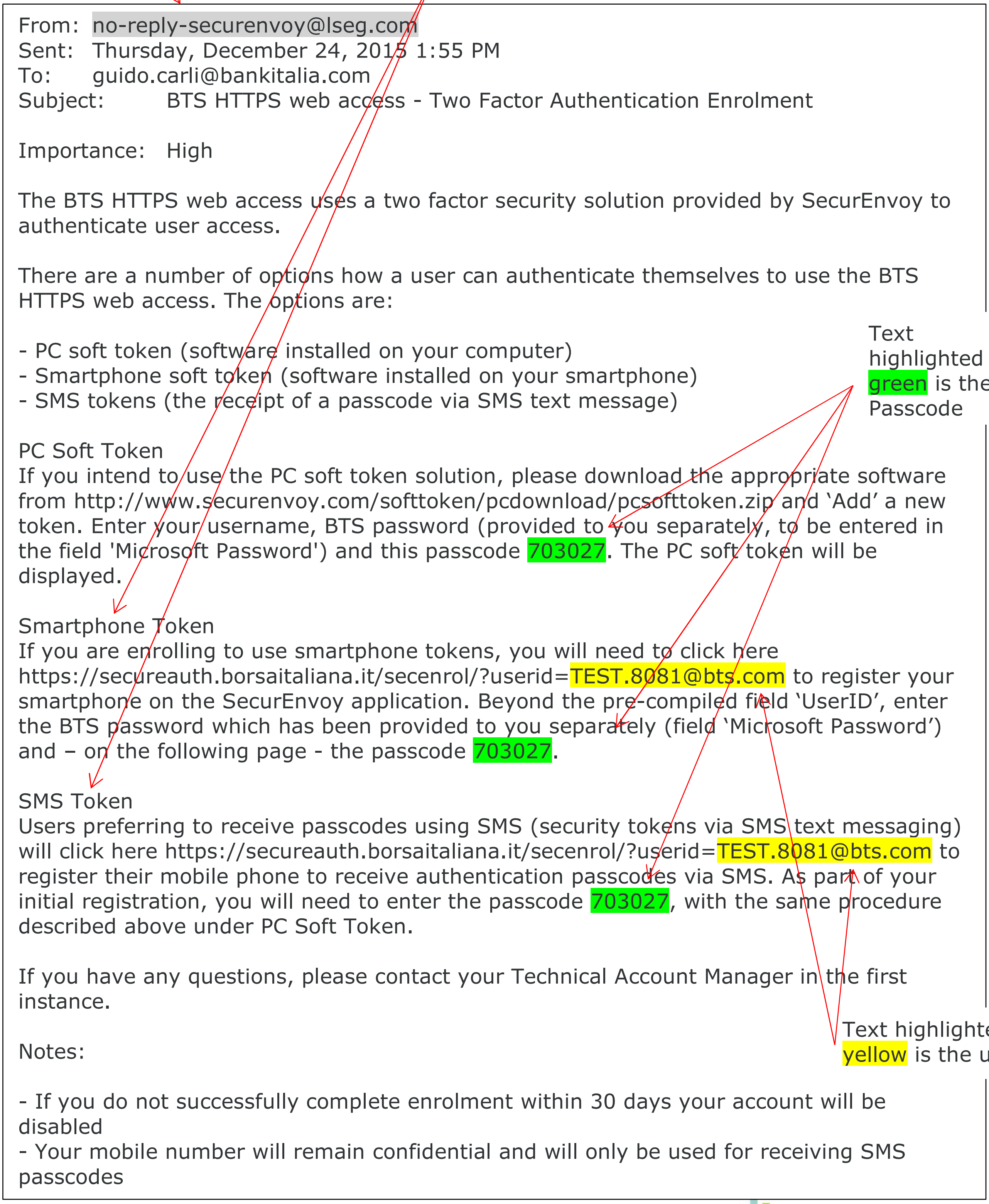
b) Provide answers to the two secret questions, which shall be used when accessing the self help desk page. Select ‘Continue’ to close the process.

c) Shortly an SMS with the first token to be used is received on the handset selected.

Example Enrolment email (Welcome Mail)

To ensure that you receive this email, please configure your spam filter to accept an email from the address highlighted in grey

A **PC soft token user** does not need to access the enrolment page, on the contrary potential problems – requiring a UserID reset – may arise in case a PC soft token user tries to access at enrolment time the enrolment page **https://secureauth.borsaitaliana.it/secenrol/** .



From: no-reply-securenvoy@lseg.com
Sent: Thursday, December 24, 2015 1:55 PM
To: guido.carli@bankitalia.com
Subject: BTS HTTPS web access - Two Factor Authentication Enrolment

Importance: High

The BTS HTTPS web access uses a two factor security solution provided by SecurEnvoy to authenticate user access.

There are a number of options how a user can authenticate themselves to use the BTS HTTPS web access. The options are:

- PC soft token (software installed on your computer)
- Smartphone soft token (software installed on your smartphone)
- SMS tokens (the receipt of a passcode via SMS text message)

PC Soft Token
If you intend to use the PC soft token solution, please download the appropriate software from http://www.securenvoy.com/softtoken/pcdownload/pcsofttoken.zip and 'Add' a new token. Enter your username, BTS password (provided to you separately, to be entered in the field 'Microsoft Password') and this passcode 703027. The PC soft token will be displayed.

Smartphone Token
If you are enrolling to use smartphone tokens, you will need to click here https://secureauth.borsaitaliana.it/secenrol/?userid=TEST.8081@bts.com to register your smartphone on the SecurEnvoy application. Beyond the pre-compiled field 'UserID', enter the BTS password which has been provided to you separately (field 'Microsoft Password') and – on the following page - the passcode 703027.

SMS Token
Users preferring to receive passcodes using SMS (security tokens via SMS text messaging) will click here https://secureauth.borsaitaliana.it/secenrol/?userid=TEST.8081@bts.com to register their mobile phone to receive authentication passcodes via SMS. As part of your initial registration, you will need to enter the passcode 703027, with the same procedure described above under PC Soft Token.

If you have any questions, please contact your Technical Account Manager in the first instance.

Notes:

- If you do not successfully complete enrolment within 30 days your account will be disabled
- Your mobile number will remain confidential and will only be used for receiving SMS passcodes

Text highlighted in green is the Passcode

Text highlighted in yellow is the userid

3.3 BTS® Logon

3.3.1 Prerequisites

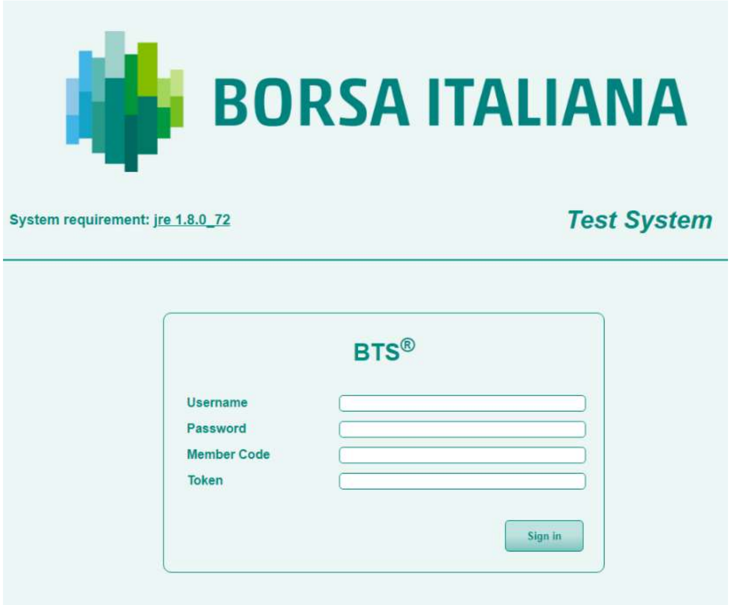
Before launching BTS® via https access, it is required to install the Java SE Runtime Environment x86, version 1.8.0_72 or later, which can be downloaded from: **http://www.oracle.com/technetwork/java/javase/downloads/java-archive-javase8-2177648.html#jre-8u72-oth-JPR** .

3.3.2 Start Application

The process is identical for both soft token and text message users.

The user must first access the Web page of the selected environment, see following table:

Environment	URL
CDS	**https://btscds.borsaitaliana.it/**
Production (Milan)	**https://btsmil.borsaitaliana.it/**
Disaster Recovery (Milan)	**https://btsmil2.borsaitaliana.it/**

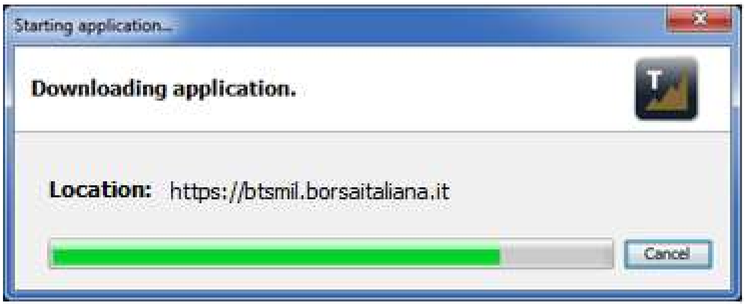


The landing page is displayed (see picture on the right).

Enter BTS® user's credentials:

- Username: BTS® user name, as provided by CTS
- Password: BTS® password, as provided by CTS
- Member Code
- Token: token displayed on the PC Soft Token, or Mobile App, or on SMS.

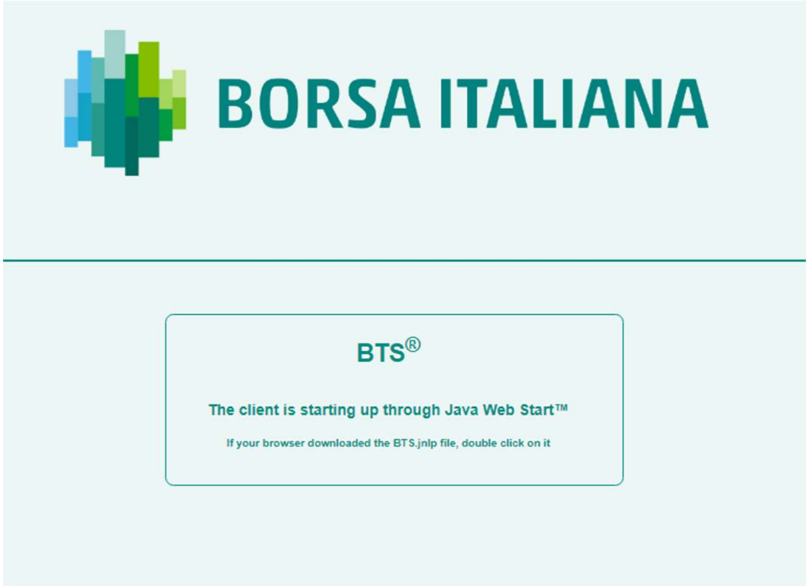
Click on 'Sign In' to finalize the authentication on BTS®.
At this point the application shall be downloaded, started and verified:



Starting application...

Downloading application.

Location: https://btsmil.borsaitaliana.it

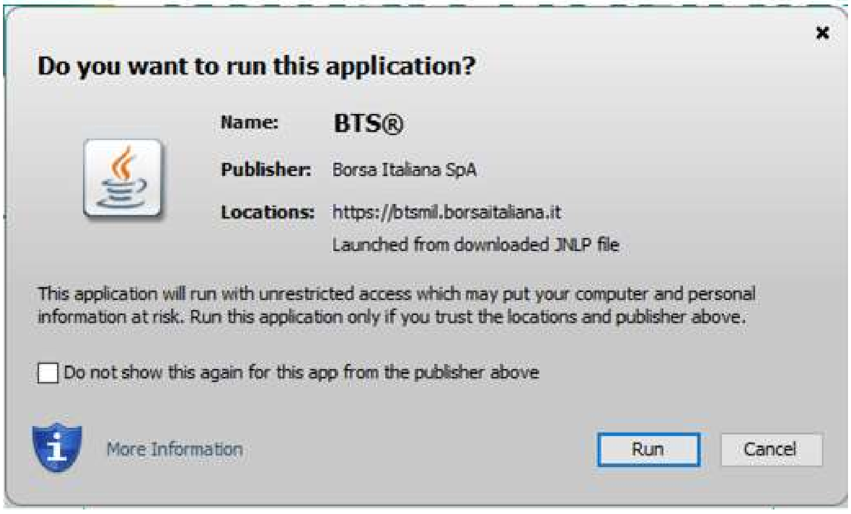


BTS®

The client is starting up through Java Web Start™

If your browser downloaded the BTS.jnlp file, double click on it

Depending on the browser configuration a confirmation to run may be asked:



Do you want to run this application?

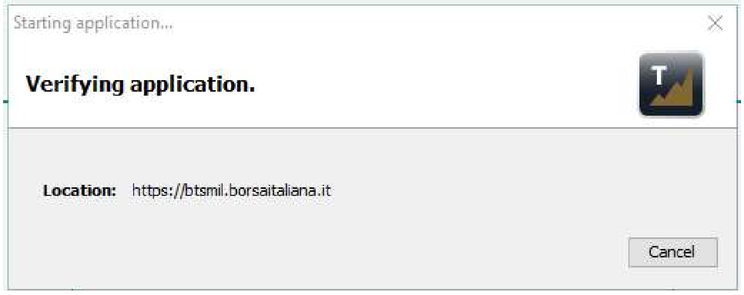
Name: BTS®

Publisher: Borsa Italiana SpA

Locations: https://btsmil.borsaitaliana.it
Launched from downloaded JNLP file

This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the locations and publisher above.

□ Do not show this again for this app from the publisher above



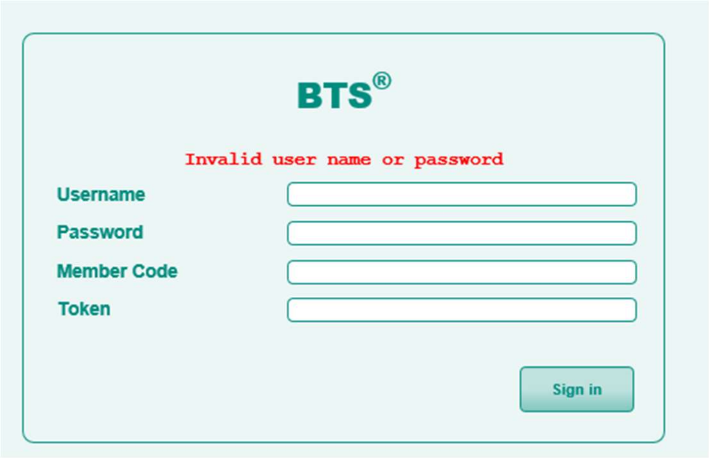
Starting application...

Verifying application.

Location: https://btsmil.borsaitaliana.it

From this point onwards please refer to the standard BTS® documentation published on Borsa Italiana web site at url: **http://www.borsaitaliana.it/borsaitaliana/gestione-mercati/bts-bittradingstation/bts.en.htm** .

To prevent concurrent access a timeout of some minutes is configured: during this timeframe a second access attempt is denied with a generic message for security reasons:



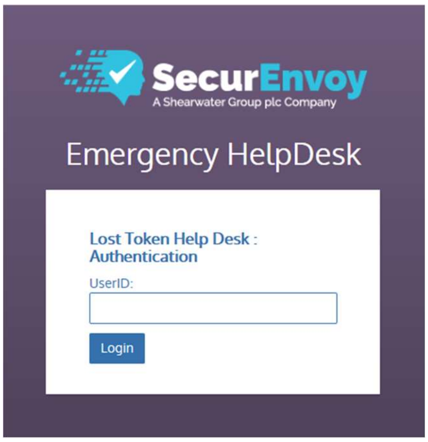
Invalid user name or password

If the timeout elapses before the process is completed, the user must re-start the whole authentication process from scratch, otherwise an error is returned.

4. TEMPORARY PASS CODES

If a user is struggling with their pass code and needs to log on quickly, they can request a temporary pass code by logging on to **https://secureauth.borsaitaliana.it/sechelpdesk** (**https://secureauth-cds.borsaitaliana.it/sechelpdesk for test environment (CDS)**:

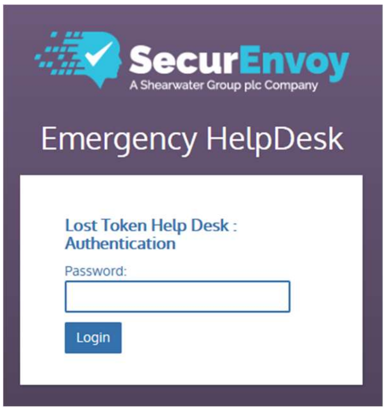
a) Enter the UserID as provided in the welcome mail (format: **userID.Member@bts.com** for production, **userID.Member@bts.test.com** for CDS). Select 'Login'


Emergency HelpDesk

Lost Token Help Desk : Authentication

UserID:

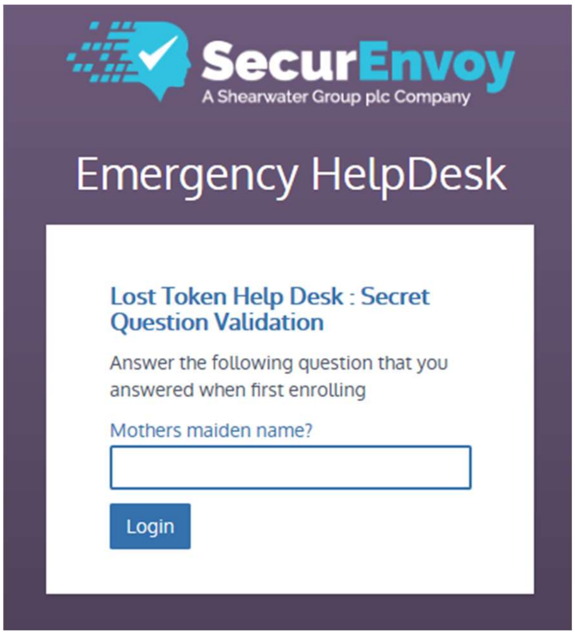
b) In the next form enter BTS® password. Select 'Login'


Emergency HelpDesk

Lost Token Help Desk : Authentication

Password:

c) One of the two secret questions provided at enrolment time is asked. Enter the answer and select 'Login'

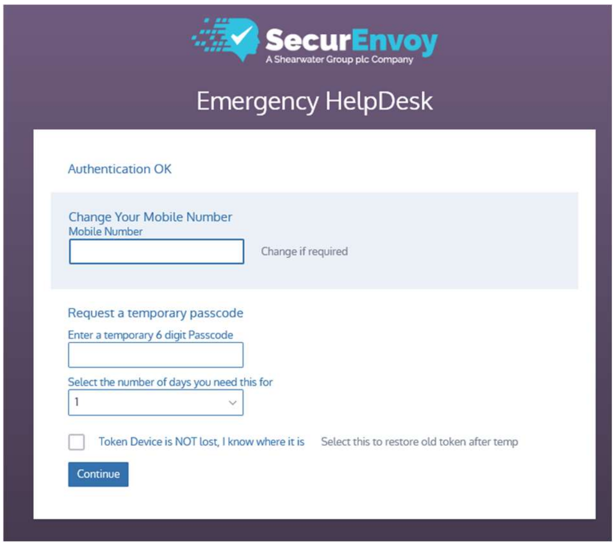

Emergency HelpDesk

Lost Token Help Desk : Secret Question Validation

Answer the following question that you answered when first enrolling

Mothers maiden name?

d) Enter (if desired) a new phone number to be used for SMS tokens and/or a Temporary Passcode, which will be in force for the number of days selected in the relevant field, Click on 'Continue' to confirm the update. User shall login on BTS® by using the passcode provided. In case a new phone number was specified please use the token sent via SMS to the new number.


Emergency HelpDesk

Authentication OK

Change Your Mobile Number

Mobile Number

Change if required

Request a temporary passcode

Enter a temporary 6 digit Passcode

Select the number of days you need this for: 1

□ Token Device is NOT lost, I know where it is — Select this to restore old token after temp

Using a temporary passcode does not require a password change.

Note that since temporary passcodes represent a security risk, to limit their use users are allowed to make one request every 30 days.

Users can also re-enrol by using temporary pass codes.

For example, text message users can re-enrol to the URL provided in the welcome email to specify a different mobile phone number.

Once re enrolment is complete, the codes sent to the mobile phone supersede the temporary passcode.

5. PASSWORD CHANGES

5.1 User Initiated Password Changes

When users change their password by own initiative no requirement to re-enrol is issued.

5.2 Forgotten Passwords

When users forget their password, they inform CTS staff who reset the account and provide the user with a new password. The account reset generates an email sent to the user with a new initial passcode.

The user must then re-enrol as described previously.

6. MOVING SOFT TOKENS BETWEEN PCs

Users can only have a single instance of a soft token (they cannot have the same soft token running on multiple PCs). If the soft token is moved between two PCs, a re-enrolment has to be performed on the destination PC.

The steps to be performed are:

- Download and install the soft token software on the new PC as described in **section 4.1** of this document
- Enrol as described in **section 4.2** of this document, but using the pass code generated by the soft token on the old PC (or if that is not available the passcode from the self-help facility, see **section 5.1**).
- Log on to BTS® using the pass code generated on the new PC. You will not be obliged to change password.
- Finally, delete the soft token on the old PC as this will no longer work.

if an organisation employs a set up under which users are allocated to different PCs each day (for example a terminal server arrangement), the soft token will not work unless it is re-enrolled daily. The options are either to bind the user to a particular terminal server, or to change from a soft token to text messages or phone/tablet app.

7. APPENDIX A SOFT TOKEN GUIDE

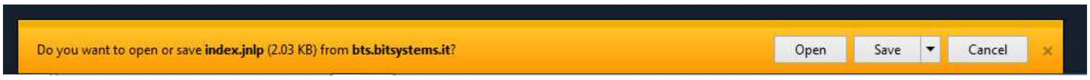
You can find Secure Envoy Soft Token Guide in the zip file
https://downloads.securenvoy.com/pcsofttoken.zip

PC Soft Token.pdf

9. APPENDIX B TROUBLESHOOTING GUIDELINES FOR JAVA WEB LAUNCHER

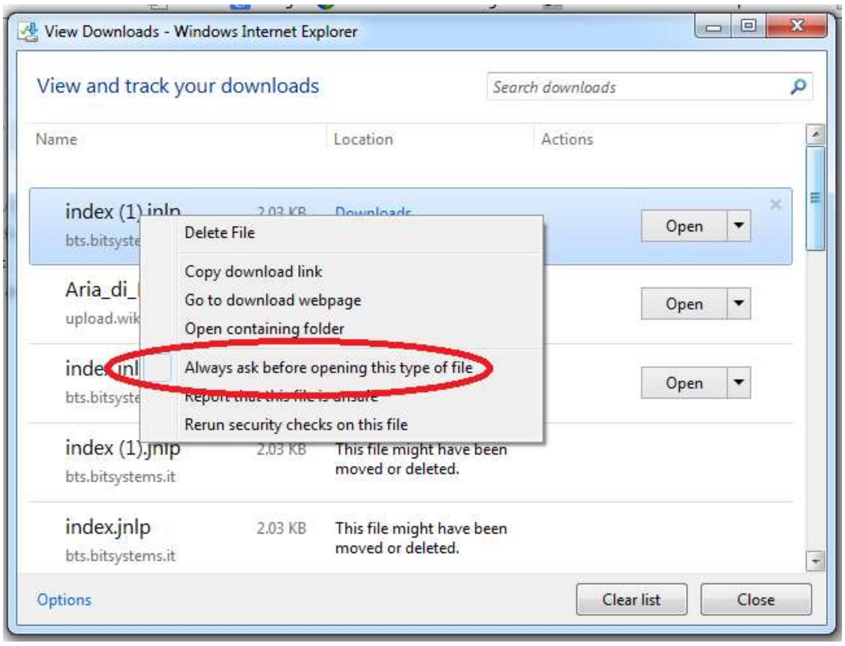
In case a pop-up appears to ask whether the selected link has to be opened or saved, follow this procedure to avoid the step in future accesses:

- **In Explorer:**
  The pop-up is displayed:

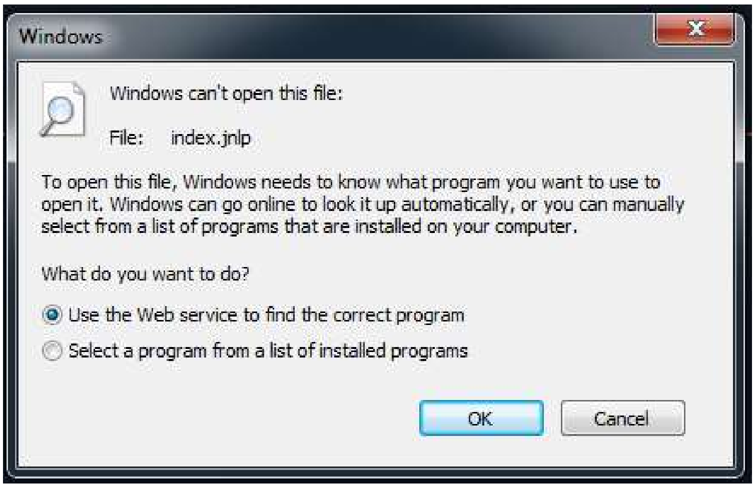


Do you want to open or save **index.jnlp** (2.03 KB) from **bts.bitsystems.it**?

1. Select the Save option.
2. Select Tools in the Menu Bar, then the View Downloads option, or click Ctrl J
3. In the popup right-click on the file that you just downloaded:



4. In the list presented, make sure to un-check the option '*Always ask before opening this type of file*'
5. In case the jnlp file extension is not associated to any application, when the '*Open* ' button is pressed, the following pop up is displayed:



Windows

Windows can't open this file:

File: index.jnlp

To open this file, Windows needs to know what program you want to use to open it. Windows can go online to look it up automatically, or you can manually select from a list of programs that are installed on your computer.

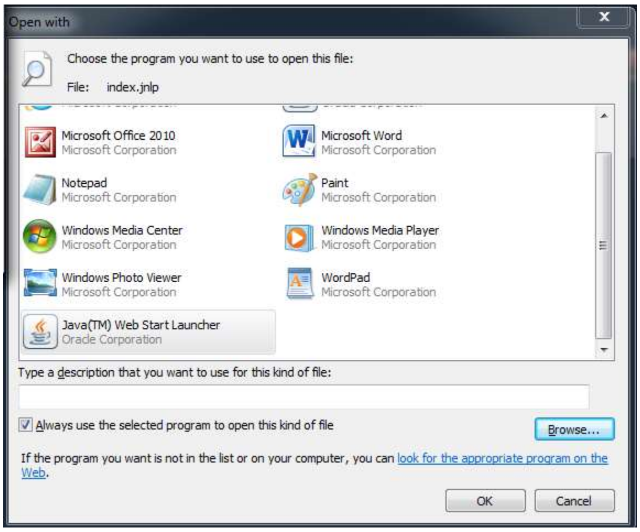
What do you want to do?

● Use the Web service to find the correct program

○ Select a program from a list of installed programs

6. Choose the option "*select a program from a list of installed programs*" and press OK.

7. From the list of programs select 'Java ™ *Web Start Launcher'*. Mind that the *'Always use the selected program to open this kind of file' tick is selected, then select OK'*:



Open with

Choose the program you want to use to open this file:

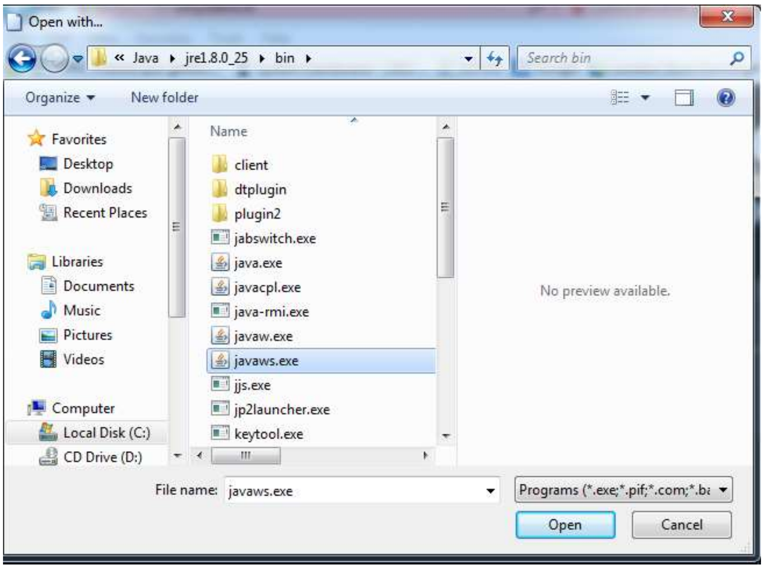
File: index.jnlp

Type a description that you want to use for this kind of file:

☑ Always use the selected program to open this kind of file

If the program you want is not in the list or on your computer, you can look for the appropriate program on the Web.

In case the application is not listed select 'Browse…'. In the pop up displayed browse in the directory containing the Java version (typically located in c:\Program Files (x86)\Java\jre1.8….\bin for 64-bit OS and x86 java version; in c:\Program Files\Java\jre1.8….\bin for 64-bit OS and x64 java version and for 32-bit OS) and select 'javaws.exe ':



Open with...

« Java ▸ jre1.8.0_25 ▸ bin ▸

No preview available.

File name: javaws.exe

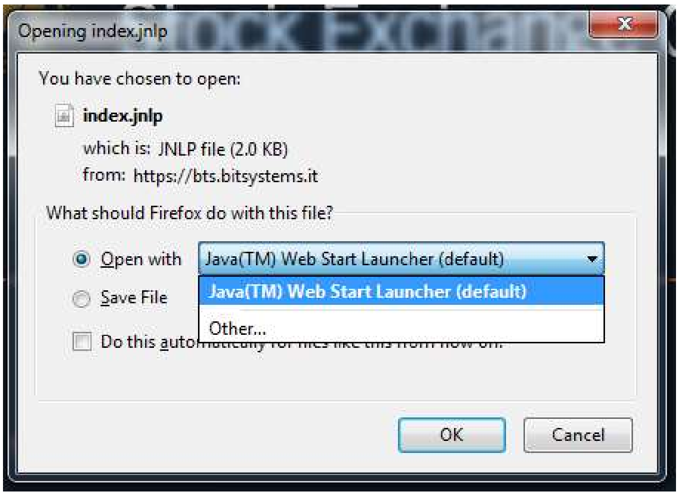
Programs (*.exe;*.pif;*.com;*.ba

Select 'Open ' and repeat step 7.

- **In Firefox:**

A pop-up is displayed:

1. Select in *'Open with'* the option '*Java ™ Web Start Launcher'*. Select the tick '*Do this automatically for files like this from now on'*. Select OK.



Opening index.jnlp

You have chosen to open:

index.jnlp

which is: JNLP file (2.0 KB)

from: https://bts.bitsystems.it

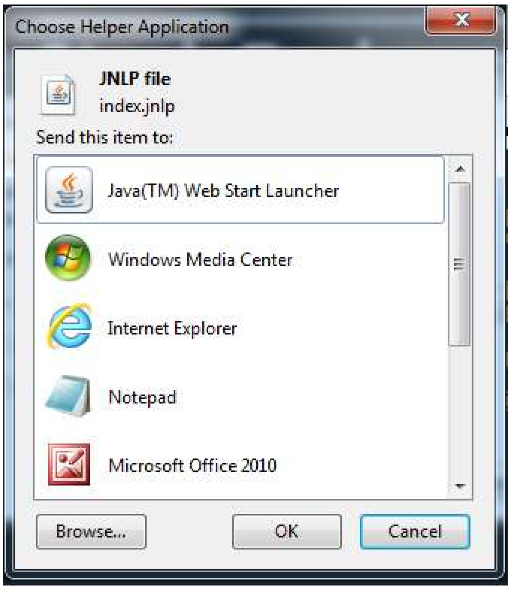
What should Firefox do with this file?

● Open with Java(TM) Web Start Launcher (default)

○ Save File

□ Do this automatically for files like this from now on.

2. In case the item is not listed select 'Other…'. From the pop up select Java ™ Web Start Launcher':



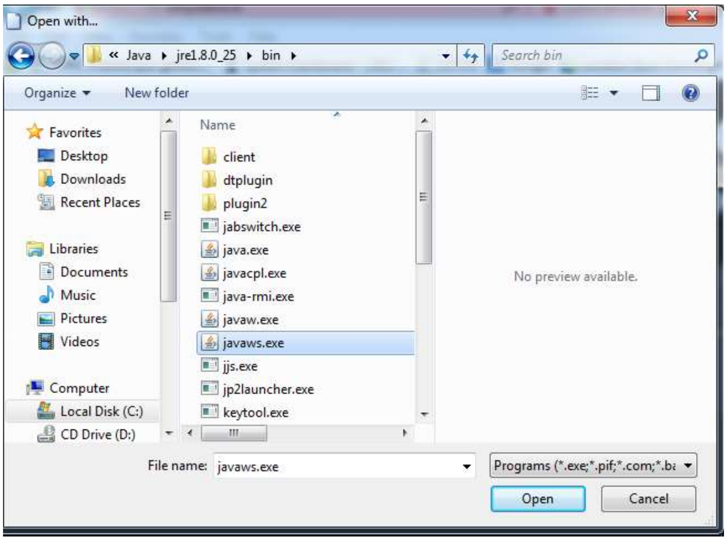
Choose Helper Application

JNLP file

index.jnlp

Send this item to:

In case the application is not listed select 'Browse…'. In the pop up displayed browse in the directory containing the Java version (typically located in c:\Program Files (x86)\Java\jre1.8….\bin for 64-bit OS and x86 java version; in c:\Program Files\Java\jre1.8….\bin for 64-bit OS and x64 java version and for 32-bit OS) and select 'javaws.exe':



File name: javaws.exe

Select '*Open*' and repeat step 2.
The association between jnlp files and Java Runtime Engine is now set.

CONTACT

Client Support

T (toll free): 0080026772000

T (from mobile): +39 02 45411399

E: Client-Support@borsaitaliana.it

Customer Relationship Management

T: +39 02 72426 512

E: clients-services@borsaitaliana.it

Disclaimer

This publication is for information purposes only and is not a recommendation to engage in investment activities. This publication is provided "as is" without representation or warranty of any kind. Whilst all reasonable care has been taken to ensure the accuracy of the content, Euronext does not guarantee its accuracy or completeness. Euronext will not be held liable for any loss or damages of any nature ensuing from using, trusting or acting on information provided. No information set out or referred to in this publication shall form the basis of any contract. The creation of rights and obligations in respect of financial products that are traded on the exchanges operated by Euronext's subsidiaries shall depend solely on the applicable rules of the market operator. All proprietary rights and interest in or connected with this publication shall vest in Euronext. No part of it may be redistributed or reproduced in any form without the prior written permission of Euronext. Euronext disclaims any duty to update this information. Euronext refers to Euronext N.V. and its affiliates. Information regarding trademarks and intellectual property rights of Euronext is located at www.euronext.com/terms-use.

EURONEXT

borsaitaliana.it