



EUROPEAN COMMISSION
DIRECTORATE-GENERAL INFORMATICS

Directorate D - Digital Services
DIGIT D3 - Trans-European Services

eTrustEx – Web version 3.2.5 User Guide

Version [1.00]

Status [Final]

© European Union, 2019

Reuse of this document is authorised provided the source is acknowledged. The Commission's reuse policy is implemented by Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents.

Date: 09/10/2019

Document Status:

Status
Draft

Document Approver(s):

Name	Role
POPGEOGIJEV Kristof	IT project officer – eTrustEx, DG DIGIT D3.002

Document Reviewer(s):

Name	Role
POPGEOGIJEV Kristof	IT project officer – eTrustEx, DG DIGIT D3.002

Summary of Changes:

0.01	03/10/2019	Anamaria BATRINU	First draft of the document based on eTrustEx Web User Guide - JavaScript version_v0.05
1.00	09/10/2019	Anamaria BATRINU	Implemented Kristof's remarks

Contents

- 1. Introduction..... 3
- 2. Definitions 3
- 3. Accessing the application 4
- 4. Compatible browsers and versions 5
- 5. Inbox..... 6
- 6. Received message details..... 7
 - 6.1. List of files section 8
 - 6.2. Downloading files 8
 - 6.3. Opening a signed message 10
 - 6.4. Decrypting the files 11
 - 6.4.1. Fill in the certificate password 12
- 7. Sending a new message 14
 - 7.1. Signing the message 16
 - 7.1.1. Signature Section..... 16
 - 7.1.2. Fill in the certificate password 17
 - 7.1.3. Certificate Validation..... 17
 - 7.2. List of files section 18
 - 7.2.1. Adding files to upload..... 18
 - 7.2.2. Uploading the files..... 20
- 8. Contact information 22

1. Introduction

This User Guide is meant to explain the functionalities of eTrustEx Web for a new User.

The screen captures included in this User Guide were taken using Google Chrome version 64. Certain fonts, components, alignments and popups might look different when using another browser or a different version of Google Chrome. The popups included in this User Guide that fall under this category are followed by an indication.

① Not applicable to e-Greffe users from section 6.3 Opening a signed message onwards.

2. Definitions

Key	Description
Party	In eTrustEx Web, the transfer of files is done Party to Party. A Party represents an organization/part of an organization/project using the eTrustEx platform in order to exchange business documents.
User	A Party can have one or more Users ; all the Users of a Party have access to the same messages received/sent by that Party . In addition, a User can have access to more Parties.
Sender	A Party which is referred to as the origin of a message sent through eTrustEx Web.
Receiver	A Party which is referred to as the recipient of a message sent through eTrustEx Web.
Interchange Agreement (ICA)	A logical communication channel, called interchange agreement is created in order to enable the communication between two Parties. This configuration is done by the eTrustEx team. Communication attributes such as confidentiality (encryption) and integrity (signature) can also be defined at the level of the ICA.
Business Administrator	In the context of eTrustEx Web, each organization/business will have at least one Business Administrator. The Business Administrator has a view on all the parties belonging to his/her business and the ability to grant Party Operator and Party Administrator roles to other Users for parties belonging to their organization/business. Additionally, Business Administrators can also change the display name of a Party as well as configure status notifications.
Party Operator	This role allows a User to view/send/receive messages in the name of a Party (or Parties) in the eTrustEx Web application.
Party Administrator	This role allows a User to view/send/receive messages in the name of a Party (or Parties) in the eTrustEx Web application and also has the ability to grant Operator and Party Administrator roles to other Users for the Party (or Parties) he/she administers in the e-TrustEx Web application.
EU Login credentials	In order to connect to eTrustEx Web, the Users need to have EU Login credentials .

Key	Description
Checksum validation	All data transfers are verified with checksums in order to avoid data corruption during transfers.

3. Accessing the application

In order to access the application you need to follow the link corresponding to the environment you need to access:

- In Acceptance: <https://webgate.acceptance.ec.europa.eu/e-trustex>
- In Production: <https://webgate.ec.europa.eu/e-trustex>

The application will display the Inbox view by default. The user can change the language by using the drop-down list in the top-right corner of the screen.

The screenshot displays the eTrustEx - Web access interface. At the top right, there is a language dropdown menu set to "English". The main header includes the European Commission logo and the text "eTrustEx - Web access Trusted Exchange Platform". Below the header, there is a navigation bar with "UROPA > European Commission > eTrustEx" and "Administration Logout". A "Party" dropdown menu is set to "ACC DECIDE TEST1 WEB PARTY" and "Logged in as: Violet".

The main content area shows an "Inbox" view with a search bar and a "Refresh" button. The messages are grouped by dossier, with the following details:

Dossier	Message Content	Received
PLAN/2019/5228	PLAN/2019/5228 - Decide - Official electronic version ACC-DECIDE-DCTEST-APP-PARTY	May 22, 2019 12:37
PLAN/2019/5221	PLAN/2019/5221 - Decide - Official electronic version ACC-DECIDE-DCTEST-APP-PARTY	May 20, 2019 11:45
	PLAN/2019/5221 - Decide - Official electronic version ACC-DECIDE-DCTEST-APP-PARTY	May 17, 2019 19:38
	PLAN/2019/5221 - Decide - Official electronic version ACC-DECIDE-DCTEST-APP-PARTY	May 17, 2019 19:34
PLAN/2019/5220		

4. Compatible browsers and versions

Once the User is accessing eTrustEx Web, if the browser used is not compatible with the application, the User will be redirected to a page showing the compatible versions.

The browser you are using is not compatible with this version of the application.

To take fullest advantage of the application we highly recommend the use of one of the compatible browsers with the minimum version specified in the table below.

Browser	Required Version	Additional information
Chrome	64	
Firefox	59	Requires the following two preferences to be enabled in about:config. -javascript.option.streams -dom.streams.enabled
Edge	17	This is the EdgeHTML version Edge is only available in Windows 10

Annotations:

- Compatible browsers and versions (points to the table)
- Additional information that might be useful or actions required (points to the Firefox row)

5. Inbox

When accessing eTrustEx Web, the User can see the received messages with the corresponding details (Subject, Sending Party, warning message about the expiration of the attachments, received date, etc.).

The User can change the Party inbox he/she is visualizing by using the Party drop-down list.

In addition, the User can search the messages by Subject and/or use the Unread filter.

The screenshot shows the eTrustEx Web interface with several callout boxes explaining its features:

- Compose a new message**: Points to the 'New' button in the Messages section.
- Refresh Inbox**: Points to the 'Refresh' button in the Messages section.
- Messages can be filtered by subject, entering a key word. The User can also see "All" messages or only the "Unread" ones**: Points to the search bar and filter tabs in the Messages section.
- Help menu containing the User Guide and the Support e-mail address**: Points to the 'Help' menu in the top right.
- Choose language**: Points to the 'English' dropdown menu in the top right.
- Important announcements**: Points to the 'Important notice for all eTrustEx users' banner at the top.
- Choose Party to see its inbox (drop down menu)**: Points to the 'Party: GUI1 NP I1C2 PARTY' dropdown menu.
- Messages can be ordered by the received date**: Points to the 'Received' column header in the message list.
- The red icon indicates that the attachments expired due to the retention policy (after 12 weeks, the attachments are not available anymore to the User)**: Points to the red warning icon next to the message 'test_20190927_1732'.
- Details about the message received: Subject (INCOMING SIGNATURE – PERMANENTLY TRUST) and Sending Party (TEST_GUI2_NP_I1C2_PARTY)**: Points to the subject and sender information of the selected message.
- Version and environment of the application**: Points to the footer text 'eTrustEx v3.2.5-3-TEST - 04-10-2019 10:06'.
- Navigate through the messages**: Points to the pagination controls '1 of 13' at the bottom right.

The warning sign can also be yellow, informing the User that the attachments will expire on a specific date

The screenshot shows the eTrustEx inbox interface. On the left, there are folders for 'Inbox(1945)', 'Sent', and 'Draft(2)'. The main area displays a list of messages. A yellow warning icon is present next to the first message, with a tooltip that reads 'Attachments are going to expire on 16/02/2018'. The messages are from 'TEST_EDMA_NP_I1C2_PARTY' and contain encrypted attachments.

6. Received message details

Once clicking on a message in the Inbox, the User can see the message details: the message subject, Sending Party ("From"), date of receiving, comments (optional field) and the list of files received.

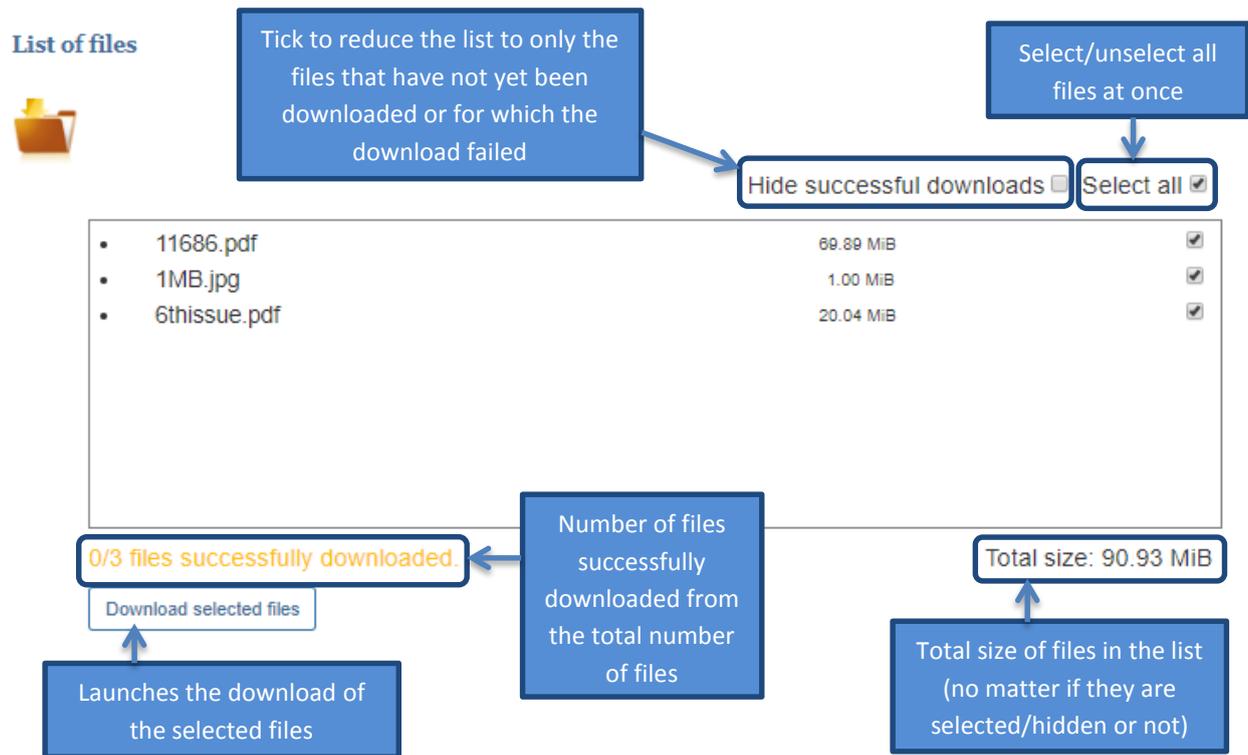
The screenshot shows the 'Received message' details page in eTrustEx. The page includes a navigation bar with the European Commission logo and 'eTrustEx - Web access Trusted Exchange Platform'. The message details are as follows:

- Subject:** 5 atta
- From:** TEST_GUI1_NP_I0C0_PARTY
- Received on:** Monday, June 18 2018 15:45
- Comments:** 5 atta
- List of files:** A table of 11 files with columns for file name, size, and a download checkbox. The total size is 61.34 MiB.

File Name	Size	Download
Вопроси заор се раќаат слободни и равни по достојност...	12.51 KiB	<input checked="" type="checkbox"/>
Η ΕΜΑδα (πολιότητα ΕΜάς), στήσιμα γυμνάσιј υς ΕΜλη...	8.55 KiB	<input checked="" type="checkbox"/>
Συνορέβι: ота Воробиткиј ме тпу Αλβανία, ота Βορσα μ...	30.13 MiB	<input checked="" type="checkbox"/>
Все люди рождаются свободными и равными в своем ...	12.51 KiB	<input checked="" type="checkbox"/>
вулкан термометр радиатор хоккей медицина цифра Ита...	12.51 KiB	<input checked="" type="checkbox"/>
остоний и западный ибеники достаточно похороки - Со...	12.51 KiB	<input checked="" type="checkbox"/>
остоний и западный ибеники достаточно похороки фокс	12.51 KiB	<input checked="" type="checkbox"/>
بھان ان اللہ ربنا ہے!!	8.55 KiB	<input checked="" type="checkbox"/>
許多那拉伯人的名字并不是其只是.txt	4.00 B	<input checked="" type="checkbox"/>

0/11 files successfully downloaded. Total size: 61.34 MiB

6.1. List of files section

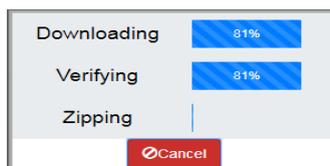


The User can select the files to download; the User can also select/deselect all the files at once by ticking/unticking the **Select all** check-box.

6.2. Downloading files

In order to download the files, the User has to click on the **Download selected files** button.

A popup window will inform the User about the progress of the download:



The files are downloaded in archives¹ of maximum 512 MiB in size. If the total size of the files is more than 512 MiB, then a new archive will be created each time this limit is reached. The archives are named following the below rules:

- Archive name starts with the sending date and time followed by the subject of the message;
- The following characters are replaced by underscores:
 - white spaces (wherever there are more than one white spaces in a row, they will be replaced by a single underscore)

¹ Archive - a compressed file containing multiple files and/or folders, created by a file archiving utility in zip format, which is a standard archive format supported by several archiving utilities (e.g. 7-Zip, WinZip, WinRAR etc.).

- special characters (e.g. " * / : < > ? \ | etc.)
- If more than one archive is created the archive names will end in _1-of-n, _2-of-n etc. where n is the total number of archives to be downloaded.

The location where the archives are placed, as well as the fact that they can be immediately opened after the download completes, is browser specific. Regarding the location, the archives can be saved in the User's Download folder or the download location configured by the User in the browser.

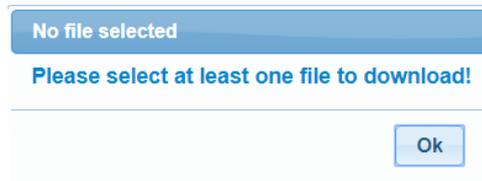
When the download is finished, the status of each file is updated, as well as the number of successfully downloaded files:

List of files

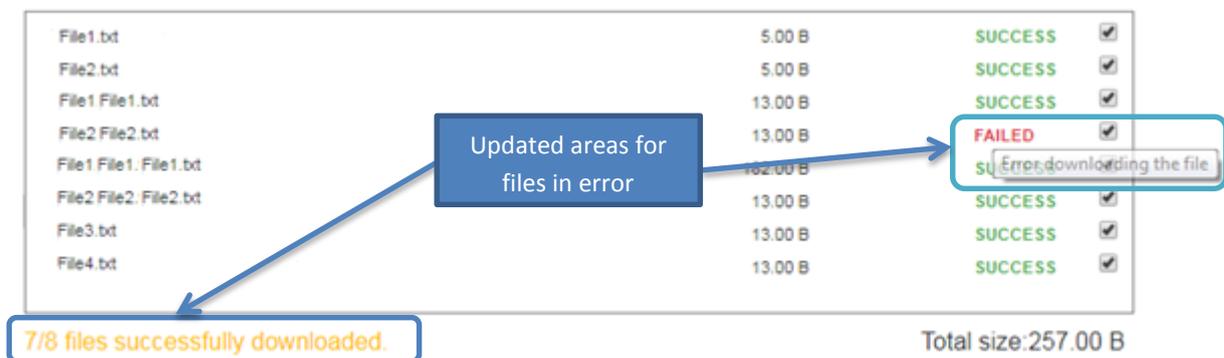


The User can download the files as many times as he/she wants.

If the User clicks on the button when no files are selected, the application will show the following popup message:

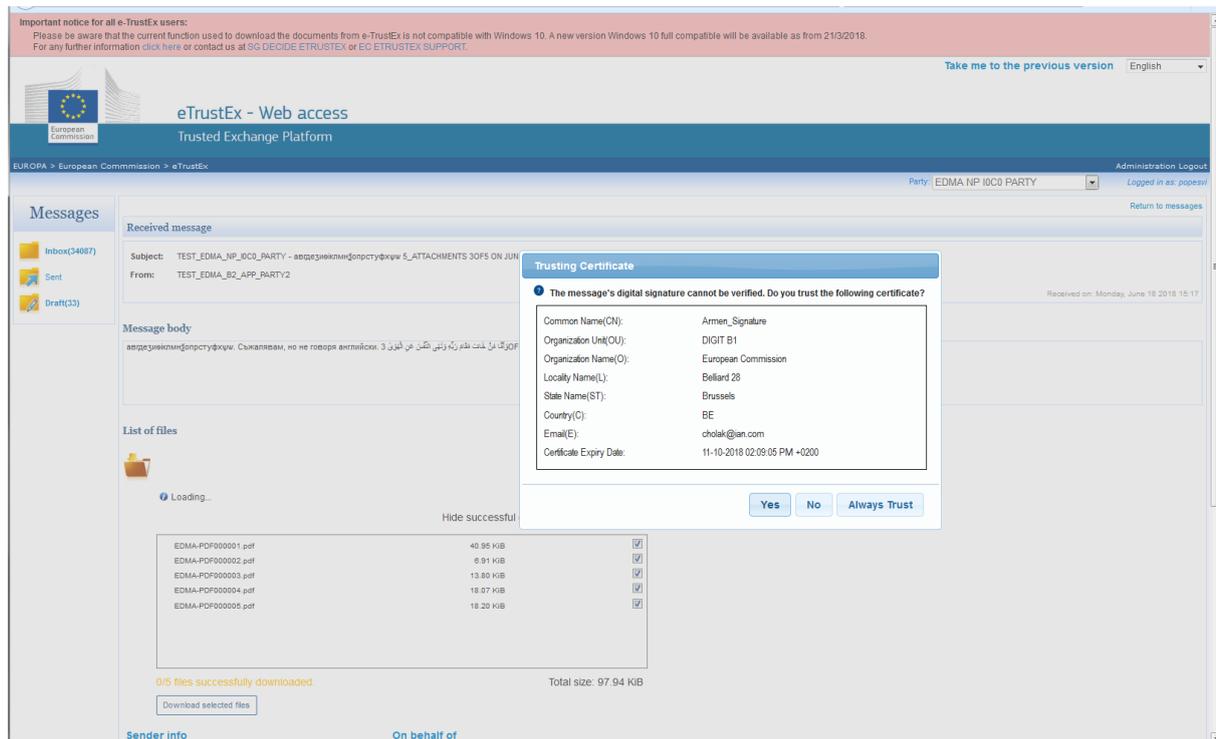


If there is an error with one of the files, the download will continue (this file will not be included in any of the archives) and its status becomes **FAILED**. Positioning the cursor over the status will display the reason of the failure.



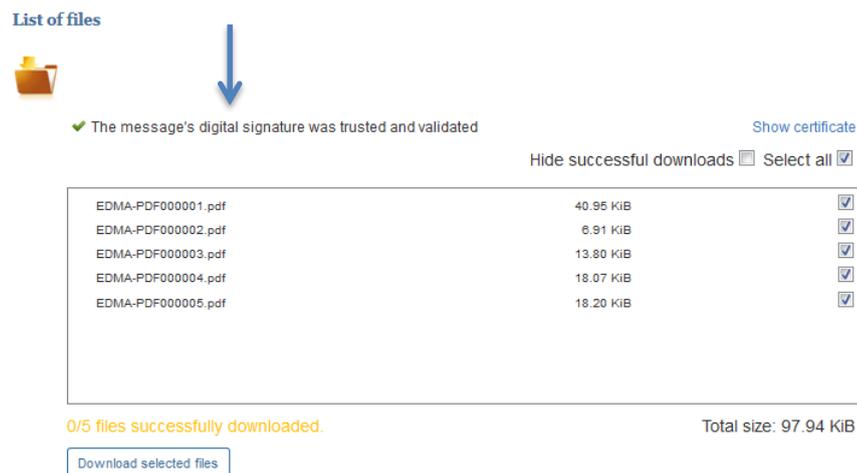
6.3. Opening a signed message

If the message was signed by the Sender, when the Receiver opens the message, the following pop-up window is shown:



The Receiver of the message is asked by the system if he/she trusts the signature certificate. The Receiver of the message has the responsibility of trusting or not the signature certificate.

If the User clicks on "Yes" or "Always trust", the following message is shown:



The difference between the two options ("Yes" and "Always trust") is that after clicking "Always trust", the application will not display anymore the pop-up window. The application will automatically trust the signature of the future messages sent by the same Party.

If the User clicks "No", the application displays the following message:

List of files

The screenshot shows a folder icon and a blue arrow pointing down. Below it is a warning message: "The message's digital signature was not trusted by the user". To the right of the warning are links for "Show certificate" and "Hide successful downloads" (unchecked) and "Select all" (checked). The file list contains five PDF files:

File Name	Size	Status
EDMA-PDF000001.pdf	40.95 KiB	✓
EDMA-PDF000002.pdf	6.91 KiB	✓
EDMA-PDF000003.pdf	13.80 KiB	✓
EDMA-PDF000004.pdf	18.07 KiB	✓
EDMA-PDF000005.pdf	18.20 KiB	✓

Below the table, it says "0/5 files successfully downloaded." and "Total size: 97.94 KiB". A "Download selected files" button is at the bottom.

If there is a problem with the signature, even if the User chooses to trust the certificate in the Trusting Certificate popup, the digital signature notification will be displayed as a warning:

The screenshot shows a warning message: "The message's digital signature was not validated". To the right are links for "Show certificate" and "Hide successful downloads" (unchecked) and "Select all" (checked). The file list contains three files:

File Name	Size	Status
11686.pdf	69.89 MiB	✓
TestJava.java	10.00 B	✓
sadhasdgh_asdjhgasd_bcdzfr_jhcbhsw_eruzsd_sauzdra...	12.30 KiB	✓

Below the table, it says "0/3 files successfully downloaded." and "Total size: 73.30 MiB".

If the checksum validation fails (e.g. the file is corrupted because of a network issue or the file was tampered etc.), the file is added to the archive renamed with the UNTRUSTED_ prefix. The status of the file becomes **UNTRUSTED** and it is not counted as a successfully downloaded file. In this case, the User should contact the Sender Party in order to send again the file and/or investigate the cause of the error.

This screenshot is annotated with blue boxes and arrows. A box around the warning "The message's digital signature was not trusted by the user" has an arrow pointing to the "UNTRUSTED" status in the file list. Another box around the "UNTRUSTED" status has an arrow pointing to a tooltip that says "Integrity check failed". A central box labeled "Updated areas when there are UNTRUSTED files" has arrows pointing to the warning, the "UNTRUSTED" status, and the "2/3 files successfully downloaded." status. The file list shows:

File Name	Size	Status
11686.pdf	69.89 MiB	SUCCESS ✓
TestJava.java	10.00 B	UNTRUSTED ✓
sadhasdgh_asdjhgasd_bcdzfr_jhcbhsw_eruzsd_sauzdra...	12.30 KiB	SUCCESS ✓

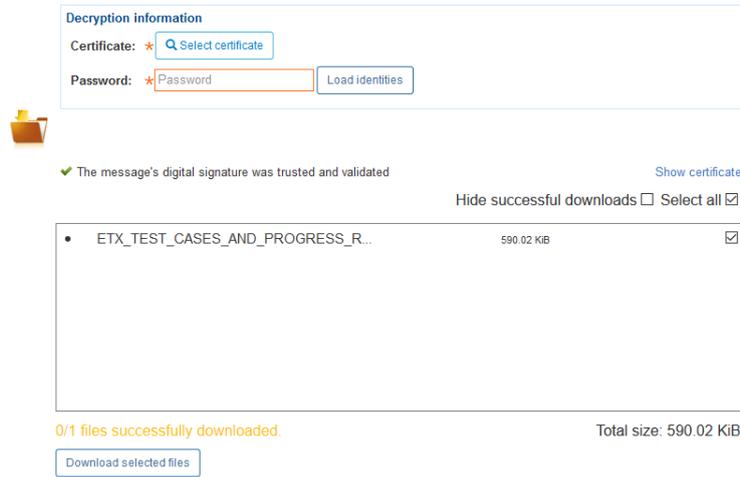
Below the table, it says "2/3 files successfully downloaded." and "Total size: 73.30 MiB".

6.4. Decrypting the files

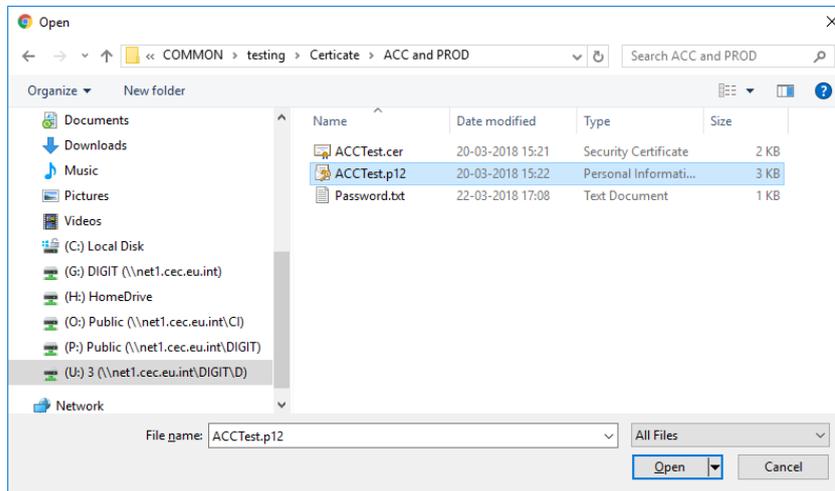
This section only concerns messages that have been sent using the recipient's public key for encryption.

In this case the list of files section will include the certificate information just above the file container:

List of files



The User has to click on the  button in order to search for and select a certificate file. The User navigates to the location of the file and selects it:



6.4.1. Fill in the certificate password

Once the User fills in the password and clicks on the  button, the system will show the information regarding the certificate's identities:

List of files

Decryption information

Certificate: * armen_key.p12

Password: *

Certificate identities:

Alias	Subject name	Valid from	Valid until
armenkey	E, ARMEN@CHOLAK.COM; C, BE; ST, BRUSSELS; L, ETTERBEEK; O, EC; OU, DIGIT; CN, ARMENKEY	25/04/2014, 09:56:15	25/04/2019, 09:56:15

 The message's digital signature was trusted and validated

Hide successful downloads Select all

- ETX_TEST_CASES_AND_PROGRESS_RE... 590.02 KiB

0/1 files successfully downloaded. Total size: 590.02 KiB

The certificate information for decryption will be validated once the User clicks on the

If the information regarding the certificate is not correct (wrong certificate or password) or is missing, the system will display the error messages above the decryption certificate information area:

List of files

Please select a valid certificate file and make sure you entered the correct password

Decryption information

Certificate: * armen_key.p12

Password: *



If the wrong certificate is provided, the User will not be able to download the files and the application will show the following message:

Wrong certificate!

Decryption failed.
The provided p12 file may not contain the correct key to decrypt the attachments of this message.

Once the User clicks , the status of the files will become **CANCELLED**:

eTrustexEncrypDecryptWF.pdf	474.70 KiB	CANCELLED <input checked="" type="checkbox"/>
-----------------------------	------------	---

0/1 files successfully downloaded.

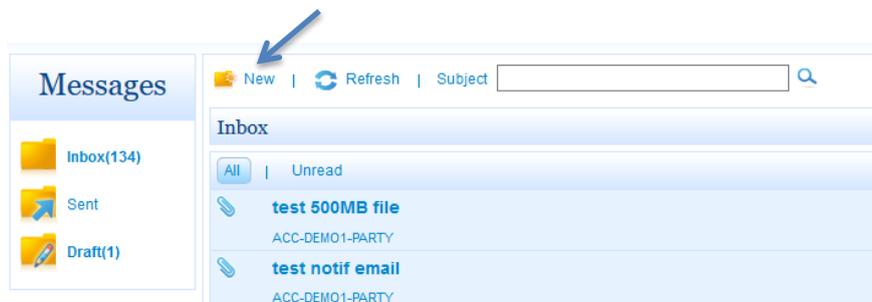
Total size:486.10 KiB

The User may now choose a different certificate and retry the download.

If the certificate and the password are correct, the status **SUCCESS** is shown for the downloaded files – please see the section **6.2_Downloading files** above.

7. Sending a new message

In order to send a new message, the User has to click on the  **New** button, located on the top left of any of the views (Inbox, Sent or Draft).



If the two Parties exchanging messages have an Interchange Agreement that allows the sending of encrypted messages (setup made by the eTrustEx Administrator), then the messages sent are automatically encrypted, without any additional action from the Sender. The levels of confidentiality are: 0 (no encryption required) and 2 (mandatory encryption).

In addition, the two Parties can exchange messages with the level of integrity 0 (optional signature) or 1 (mandatory signature).

Once clicking on the  **New** button, the below screen is shown and the User can choose the Sending Party ("To"), fill in the subject, add comments and upload the files.

The User can also check the box "Sign the message". In the below example, the signature is optional (integrity level is 0).

Optional signature: the User has to check the signature box in order to sign the message

English

The screenshot shows the 'eTrustEx - Web access' interface. At the top, there is a header with the European Commission logo and the text 'Trusted Exchange Platform'. Below this, a navigation bar shows 'EUROPA > European Commission > eTrustEx'. On the right, there is a language dropdown set to 'English' and a 'Party' dropdown set to 'EDMA NP IOCO PARTY'. The main content area is titled 'Messages' and contains a 'New' message form. The form has fields for 'To:' (filled with 'TEST_EDMA_B2_APP_PARTY2'), 'Subject:' (with an empty text box), and 'Signature:' (with a checkbox labeled 'Sign the message'). Below the form is a large empty text area for the 'Message body'. At the bottom, there is a 'List of files' section with a folder icon, a text box for file names, and buttons for '+ Add files', '+ Add folder', 'Start upload', and 'Remove all files'. The status shows 'Files to upload: 0', 'Total files: 0', and 'Total size: 0.00 B'.

The User fills in the subject of the message

The User can optionally add comments to the new message

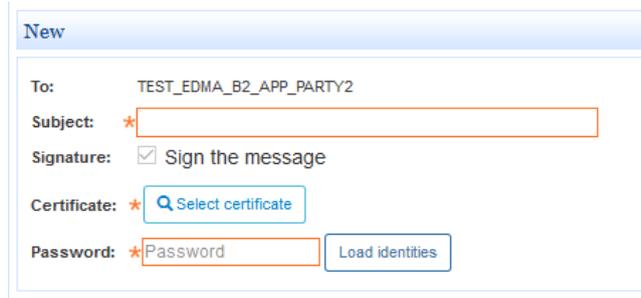
The User adds files in the "List of files" section

7.1. Signing the message

7.1.1. Signature Section

Signing a message can be optional or mandatory. The integrity (signature) level is defined when the eTrustEx Administrator is setting up the Interchange Agreement between the two Parties. The User interface and interaction when the signature is optional or mandatory is slightly different.

If the signature is required, the User will see the following fields in the "New" message view (the Signature check-box is ticked by default and the User cannot change it).

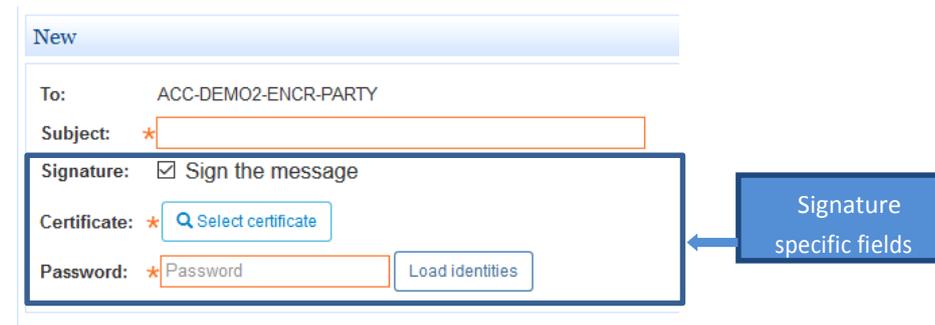


The screenshot shows a form titled "New" with the following fields: "To: TEST_EDMA_B2_APP_PARTY2", "Subject: * [text input]", "Signature: Sign the message", "Certificate: * [Select certificate button]", and "Password: * [password input] [Load identities button]".

If the signature is optional, the User will only see the Signature check-box which is unticked. If the User wants to sign the message, the User has to tick the check-box and the other certificate fields will be displayed.

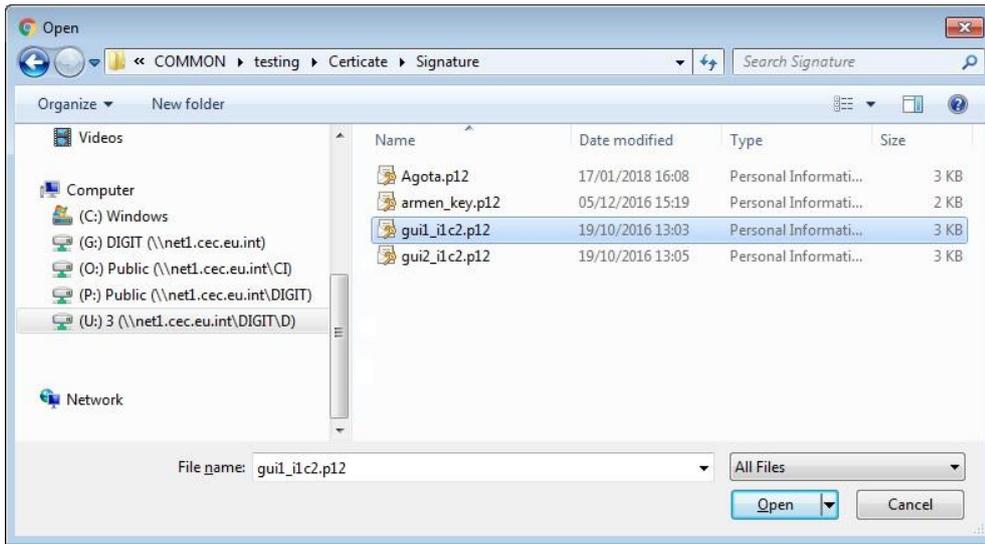


The screenshot shows a form titled "New" with the following fields: "To: TEST_EDMA_B2_APP_PARTY2", "Subject: * [text input]", and "Signature: Sign the message". A blue callout box with the text "Tick the box in order to sign the message" has an arrow pointing to the signature check-box.



The screenshot shows a form titled "New" with the following fields: "To: ACC-DEMO2-ENCR-PARTY", "Subject: * [text input]", "Signature: Sign the message", "Certificate: * [Select certificate button]", and "Password: * [password input] [Load identities button]". A blue callout box with the text "Signature specific fields" has an arrow pointing to the Signature, Certificate, and Password sections.

The User has to click on the [Select Certificate](#) button in order to search for and select a certificate file. The User then has to navigate to the location of the certificate file and select it:



7.1.2. Fill in the certificate password

Once the User fills in the password and clicks on the  button, the system shows the information regarding the certificate’s identities:

New

To: ACC-DEMO2-ENCR-PARTY

Subject: *

Signature: Sign the message

Certificate: * armen_key.p12

Password: *

Certificate identities:

Alias	Subject name	Valid from	Valid until
armenkey	E, ARMEN@CHOLAK.COM; C, BE; ST, BRUSSELS; L, ETTERBEEK; O, EC; OU, DIGIT; CN, ARMENKEY	25/04/2014, 09:56:15	25/04/2019, 09:56:15

7.1.3. Certificate Validation

The certificate information will be validated once the User clicks on the  button. If the User fills in a wrong certificate or password or does not fill in these two fields, the error messages resulting from

 Save |  Send |  Cancel

Certificate password is mandatory.

New

To: ACC-SANITY-GUI2 -NP-I1C2-PARTY

Subject: *

Signature: Sign the message

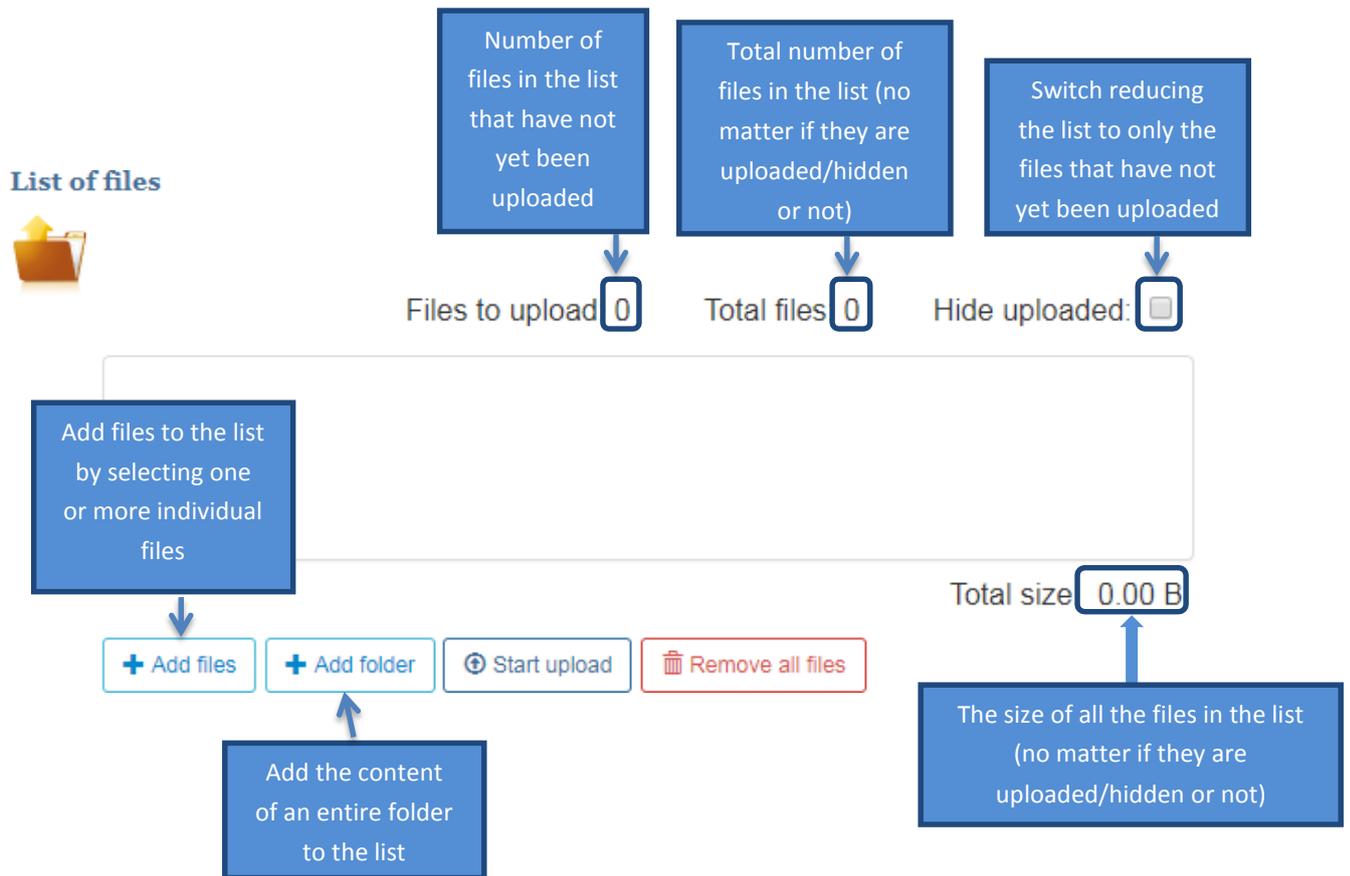
Certificate: * armen_key.p12

Password: *

this validation are displayed at the top of the page, as shown in the following example:

7.2. List of files section

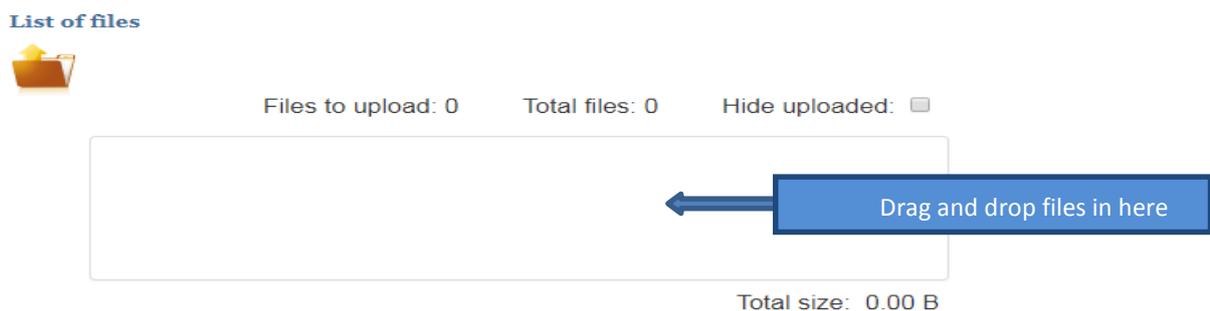
The User can add files to a message in the “List of files” section. The features available within the “List of files” section are explained below:



7.2.1. Adding files to upload

The User can add files to the list of files in three ways:

1. Drag and drop the files or the folders containing the files to the file area (all the files in the folder and all its subfolders are added to the list recursively):

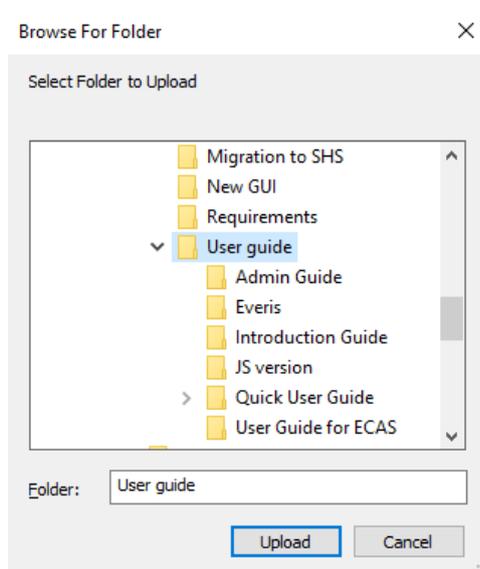


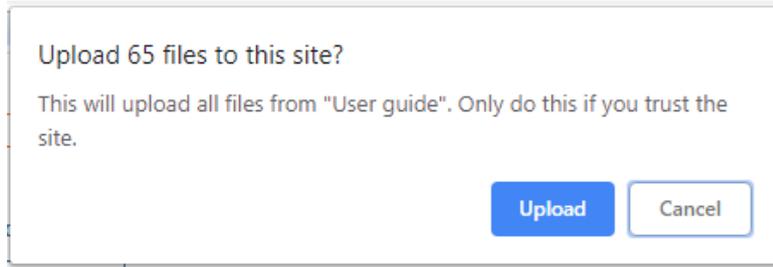
2. Via the  button, the User can add one or more individual files:



The above popup might vary based on the browser used and its version.

3. Via the  button, the User can add all the files from a selected folder, keeping the folder structure (it will also add the files from any subfolder):

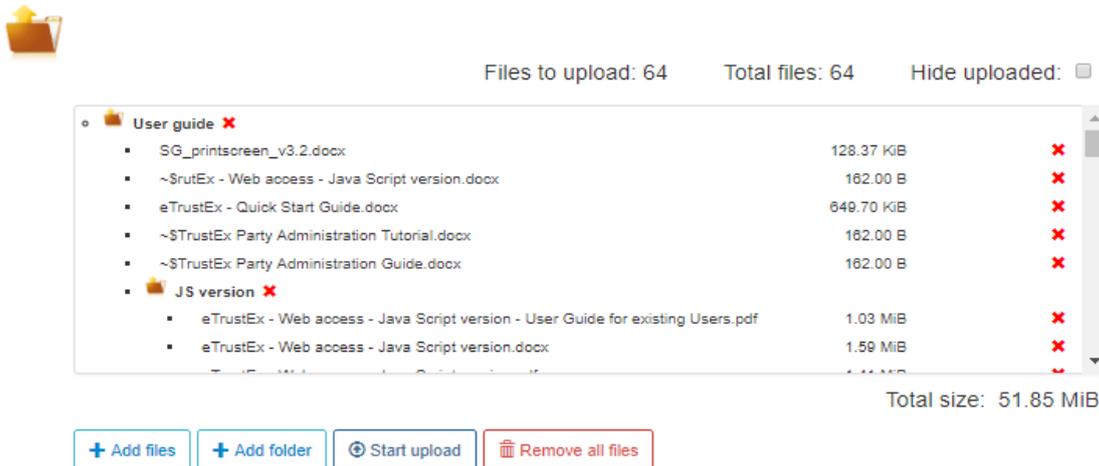




The above popups might vary based on the browser used and its version (some browsers will not display the second popup at all). Clicking on the **Upload** button in this popup will add the files to the list of files that need to be uploaded, keeping the tree-display of the folder.

The files will be then displayed in the list of files with no status associated. The User will be informed about the status of the files uploaded (“Success” or “Failed”) only after clicking on the **Start upload** button. In the following example, the User added a folder with structure for the upload.

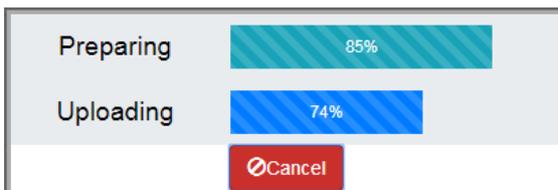
List of files



The User can remove any of the files or the whole folder by using the **Remove all files** button or all the files at once by using the **Remove all files** button.

7.2.2. Uploading the files

In order to upload the files in the list, the User has to click on the **Start upload** button.



A popup showing the progress of the upload will appear on the screen:

If the User chooses to cancel the upload, the following progress bar will be shown while the cancellation is being executed (only the files that have not yet been uploaded will be cancelled – they will appear in

8. Contact information

For more information, please contact the eTrustEx Support Team, at EC-ETRUSTEX-SUPPORT@ec.europa.eu Standard Service: 8am to 6pm (normal EC working Days).