|  |  |  |  |
| --- | --- | --- | --- |
|  | **European Commission**  **DIRECTORATE GENERAL**  <INFORMATICS> | **logo RUP@EC-Fixed-v1** |  |

Select Destination Party when Creating New Messages

|  |  |
| --- | --- |
| Author | Anamaria BATRINU (DIGIT-EXT) |
| Created | 04/09/2017 |
| Last Updated | 06/09/2017 |

**Summary of Changes**

Changes to this document are summarized in the following table in reverse chronological order (latest version first).

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Created by** | **Short Description of Changes** |
| **0.01** | **04/09/2017** | **BATRINU Anamaria (DIGIT-EXT)** | **First draft based on** ETXWEB-CR2016-07 (see JIRA [ETX-1988](https://webgate.ec.europa.eu/CITnet/jira/browse/ETX-1988)) |
| **0.02** | **07/09/2017** | **BATRINU Anamaria (DIGIT-EXT)** | **Update following comments from developers** |
| **0.03** | **08/09/2017** | **BATRINU Anamaria (DIGIT-EXT)** | **Update following the clarification of the difference in storing and using Certificate (Web vs. Node)** |
| **0.04** | **12/09/2017** | **BATRINU Anamaria (DIGIT-EXT)** | **Added information on Integrity level in section 7** System builds and sends the message |

**Configuration Management: Document Location**

The latest version of this controlled document is stored in [[this location].](https://webgate.ec.europa.eu/CITnet/svn/ETX/etrustex/trunk/etrustex/docs/Requirements)

Contents

[Use Case Description 4](#_Toc493493901)

[Actors 4](#_Toc493493902)

[Basic Flow 4](#_Toc493493903)

[1. User wants to open the New message page 4](#_Toc493493904)

[2. System displays the New message page 4](#_Toc493493905)

[3. User chooses the desired destination party from the "To: " drop-down list. 5](#_Toc493493906)

[4. System loads the corresponding interchange agreement 5](#_Toc493493907)

[5. Other intermediary User/System steps that are not subject of this change may be performed 5](#_Toc493493908)

[6. User clicks Send () 5](#_Toc493493909)

[7. System builds and sends the message 5](#_Toc493493910)

[Sub Flow 5](#_Toc493493911)

[S1. Encryption change 5](#_Toc493493912)

[Alternate Flow 6](#_Toc493493913)

[A1. At step 6 User clicks Send () , user clicks Save () 6](#_Toc493493914)

[A2. At step 5 Other intermediary User/System steps that are not subject of this change may be performed, user changes the Receiver party selection 6](#_Toc493493915)

[A3. At any step, User clicks Cancel in the New message page 6](#_Toc493493916)

[Exceptional Flow 6](#_Toc493493917)

[E1. At any step, a technical error occurs 6](#_Toc493493918)

[Prerequisites 6](#_Toc493493919)

[Additional Information 6](#_Toc493493920)

[Drop-down interaction 6](#_Toc493493921)

[Default selection 6](#_Toc493493922)

[First selection 6](#_Toc493493923)

[Selection change 6](#_Toc493493924)

[User interface 7](#_Toc493493925)

# Use Case Description

e-Trustex Web Access does not currently allow the user to choose the receiver party to which the messages are sent. It is a limitation that needs to be removed, and this Use Case describes the new desired behaviour.

# Actors

|  |  |
| --- | --- |
| Actors | Description |
| Sender Party | The Party sending the message. |
| Receiver Party | The Party receiving the message. |
| System | e-Trustex Web Access |
| User | A human accessing the System. |

# Basic Flow

## User wants to open the New message page

User wants to open the **New** message page. There are two ways of doing this:

* Any mail box (Inbox/Sent/Draft) > New ()
* Draft () > Click on a draft message

The only difference is that the first option will open an empty New message page, whilst the second will open a New message page with, potentially, some data already filled in.

## System displays the New message page

Current:

**"To:** **"** field is automatically filled in with a hard-coded party and cannot be changed.



Desired:

* If there is only one ICA with the currently selected Sender party, the **"To:** **"** field is represented as plain text.



* Otherwise, **"To:** **"** field is represented by a drop-down list, with no default selection. The list is populated with all parties having an ICA with the currently selected Sender party (top right of the page).

Refer to *Default selection* section for more details on how the component should behave.

## User chooses the desired destination party from the "To: " drop-down list.

Refer to *First selection section* for more details on how the component should behave.

## System loads the corresponding interchange agreement

System uses the information corresponding to this interchange agreement in order to know if the attachments and the message need to be sent encrypted (ICA Confidentiality level 2 means encryption is mandatory), and if the message needs to be signed (ICA Integrity level 2 means signing is mandatory).

## Other intermediary User/System steps that are not subject of this change may be performed

E.g.: filling in other fields, uploading files or folder, signing the files etc.

## User clicks Send ()

## System builds and sends the message

System validates the information: the Destination party (**"To:"** field) is not empty.

System asks User if the message needs to be signed before sending and will apply the signature. Signing becomes compulsory, if the Integrity level of the ICA is higher than MODERATE. This needs to be checked as the ICA changes once a different Receiver has been selected and the Integrity level might also change.

Depending on the Confidentiality level of the ICA between the sender and the selected receiver party the message may be encrypted or not. Before, this ICA was always known, as the receiver party was hard-coded. Now the ICA is reloaded on receiver change.

# Sub Flow

## S1. Encryption change

The User is warned (via a dialog) that currently uploaded files will be disregarded and new uploads are necessary.

The following choices are given to the User:

* Accept and Confirm the action, in which System clears the list of added files and User will need to start over the upload of the files he/she needs
* Cancel the action, in which case he/she is returned to the New message page which is in the same state as before the warning was presented to the User

# Alternate Flow

## A1. At step 6 User clicks Send () , user clicks Save ()

User clicks **Save**.

System saves the information that has been provided up to this point. No validation is performed, so a completely blank message can be saved.

## A2. At step 5 Other intermediary User/System steps that are not subject of this change may be performed, user changes the Receiver party selection

Refer to *Selection change section* for more details on how the component should behave.

## A3. At any step, User clicks Cancel in the New message page

User is returned to the **Inbox** page.

# Exceptional Flow

## E1. At any step, a technical error occurs

In case of a technical error, System displays an error page to the user. The information introduced and not saved by the User is lost.

# Prerequisites

**User** has the appropriate rights to access the **System** and perform the actions in this use case.

# Additional Information

## Drop-down interaction

### Default selection

While no Receiver Party has been chosen, the Open Upload button is disabled.

### First selection

Once a Receiver Party is selected, the Open Upload button is enabled.

### Selection change

Each time the Receiver Party selection is changed, System reloads the interchange agreement corresponding to the new selection.

If no file was uploaded before the selection change, System does not need to take any extra action.

In the case the User already uploaded some files and then changed the selection the following cases may arise (concerning the File Upload), depending on the Confidentiality level in the interchange agreements:

#### Same Confidentiality level

The Confidentiality level of the Interchange Agreement corresponding to the new selection is the same as the one corresponding to the previous selection.

If Confidentiality level is PUBLIC, System does not need to take any extra action, as no encryption was done and no encryption is needed.

If the Confidentiality level is LIMITED\_HIGH, the System checks the certificate corresponding to the ICA of the newly selected Receiver and the one corresponding to the ICA of the previously selected one by using the certificate's serial number and issuer. There are two possibilities:

* Identical certificates: System does not need to take any extra action, as the files were encrypted with the same certificate.
* Different certificates: the files need to be encrypted with the certificate corresponding to the ICA of the new Receiver (include sub flow S1. Encryption change )

#### Different Confidentiality level

In this case one Confidentiality level is PUBLIC and the other is LIMITED\_HIGH.

* PUBLIC > LIMITED\_HIGH: the files that previously were not encrypted must now be encrypted (include sub flow S1. Encryption change )
* LIMITED\_HIGH > PUBLIC: the files that previously were encrypted must now not be encrypted (include sub flow S1. Encryption change )

### User interface

|  |  |
| --- | --- |
| Default (collapsed) |  |
| Expanded |  |
| Selected (collapsed) |  |
| Selected (expanded): empty choice not available |  |