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

**e-TrustEx - Use Case Specification: User Access**

|  |
| --- |
| *---- Remove this text box after reading ---*  Help text for this Artifact Template Version 2012-01  ***Key to symbols used in this template:***  *[] indicates text to be replaced by the user of this template.*  *<> indicates text that is updated using Document Properties button.*  ***Click here to update the Document Properties >>***   * *This button is also available on the next page.*   ***Other information:***   * *Check that you are using the latest template* –[click](http://www.cc.cec/RUPatEC/) * *While working on the document, you may choose to leave some of the blue text guidance.* |

**Document Control Information** 

|  |  |
| --- | --- |
| **Settings** | **Value** |
| **Directorate:** | <INFORMATICS> |
| **Project Name:** | e-TrustEx |
| **Document Author:** | Alice Vasilescu |
| **System Owner:** | Tanya Chetcutti |
| **Project Manager:** | Tanya Chetcutti |
| **Revision Status:** | Draft |
| **Sensitivity:** | Limited DG |
| **Issue Date:** | <Issue Date> |

**Document Approver(s):**

(All Approvers are required. Records of each approver must be maintained.)

|  |  |
| --- | --- |
| **Approver Name** | **Role** |
| [Name] | [Role] |
|  |  |
|  |  |

**Document Reviewers:** (Records of each required reviewer must be maintained.)

|  |  |
| --- | --- |
| **Reviewer Name** | **Role** |
| [Name] | [Role] |
|  |  |
|  |  |

NOTE: All Reviewers in the list are considered required unless explicitly listed as Optional.

**Summary of Changes:**

The Document Author is authorized to make the following types of changes to the document without requiring that the document be re-approved:

* Editorial, formatting, and spelling
* Clarification

To request a change to this document, contact the Document Author or Owner.

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** |
| [0.1] | [06/21/2013] | [Alice Vasilescu] | [Initial Version of approved document] |
| [0.2-0.3] | [09/25/2013] | [Alice Vasilescu] | [Internal review] |
|  |  |  |  |

**Configuration Management: Document Location**

The latest version of this controlled document is stored in [this location].

Contents

[1. Use-Case Description 4](#_Toc391299531)

[1.1. Functional Features List 4](#_Toc391299532)

[2. Flow of events 5](#_Toc391299533)

[2.1. B1: Basic Flow 5](#_Toc391299534)

[2.1.1. User initiates a secure session with the System 5](#_Toc391299535)

[2.1.2. System requires User authentication 5](#_Toc391299536)

[2.1.3. Use provides credentials to System 5](#_Toc391299537)

[2.1.4. System checks authentication data 5](#_Toc391299538)

[2.1.5. System authenticates user 5](#_Toc391299539)

[2.1.6. System checks the integrity of the XML message 5](#_Toc391299540)

[2.1.7. System checks if the authenticated User can be authorised to access the services 5](#_Toc391299541)

[2.2. Subflows 6](#_Toc391299542)

[2.3. Alternative Flows 6](#_Toc391299543)

[2.4. Exceptional Flows 6](#_Toc391299544)

[2.4.1. E1: At step 2.1.4 “System checks authentication data”, the authentication data is incorrect 6](#_Toc391299545)

[2.4.2. E2: At step 2.1.4 “System checks authentication data”, the http authentication header is missing 6](#_Toc391299546)

[2.4.3. E3: At step 2.1.6 “System checks the integrity of the XML message”, the message Body does not contain only one direct child element 6](#_Toc391299547)

[2.4.4. E4: At step 2.1.5 “System checks the integrity of the XML message”, the operation XML wrapper element does not contain one and only one element 6](#_Toc391299548)

[2.4.5. E5: At step 2.1.4 “System checks authentication data”, and the digital signature is missing 6](#_Toc391299549)

[2.4.6. E6: At step 2.1.4 “System checks authentication data”, and the certificate used for the digital signature is not trusted 7](#_Toc391299550)

[2.4.7. E7: At step 2.1.4 “System checks authentication data”, and the validation of the digital signature fails 7](#_Toc391299551)

[3. Special requirements 7](#_Toc391299552)

[3.1. Interface(s) with other Systems 7](#_Toc391299553)

[3.2. Security Requirements 7](#_Toc391299554)

[3.3. Other Non Functional Features 7](#_Toc391299555)

[3.4. Constraints 7](#_Toc391299556)

[4. Preconditions 7](#_Toc391299557)

[4.1. Precondition One 7](#_Toc391299558)

[4.2. Precondition Two 7](#_Toc391299559)

[5. Post conditions 7](#_Toc391299560)

[5.1. Post condition one 7](#_Toc391299561)

[6. Additional information 8](#_Toc391299562)

[6.1. Additional links 8](#_Toc391299563)

# Use-Case Description

The system supports Synchronous User Access Control services (e.g. via web services).

In the context of this Use Case, four concepts need to be explained:

- Authentication constitutes the process of verifying the claimed identity of a User. The factors used for the authentication are the User’s username and password.

- Read authorization constitutes granting access to the system read services and Document Wrapper services based on the User’s Sender Party Agreement derived from the User identity and Sender Party ID.

- Write authorization constitutes granting access to the system write services based on the User’s profile linked to the Interchange Agreement derived from the Sender Party Agreement and Receiver Party ID.

- The Party (Sender/Receiver) ID is defined by the Sender/Receiver Identifier element and its schemeID attribute. The Party (Sender/Receiver) ID is the concatenation of the Identifier schemeId attribute, the ‘#‘ character separator and the element value. If the schemeId is null, only the element value is used as Party ID.

For example:

<urn1[[1]](#footnote-1):Identifier schemeId = "VAT">123456789</urn1: Identifier>

Gives a Party ID equals to VAT#123456789

<urn1: Identifier >123456789</urn1: Identifier>

Gives a Party ID equals to 123456789

An important point to note is that the eTrustEx data model supports only one identifier per Party .

# Functional Features List

*Security* Logging of logons, transactions, checks and other actions

*Security* Data integrity during message exchange

*Security* Authenticity of destination.

*Security* Data confidentiality during message exchange

*Security* Restricted access to services via the support of user profiles

*Security* Restricted access to the system by authentication of Users

*Security* Support of bilateral agreements to manage access to system services

*Security* Rejection notifications without introducing security vulnerabilities

*Data* Support of EAN numbers to identify the Party entity

*Security* Restricted access to data based on the ownership of the data item

*Security* Locking of user accounts

*Data* Support of different type of Party Identifier

# Flow of events

# B1: Basic Flow

# User initiates a secure session with the System

* This use case starts after the User has initiated a connection to an e-TrustEx service end-point

# System requires User authentication

* The System accepts the secure connection and asks the User to provide authentication data

# Use provides credentials to System

* The User provides username and password

# System checks authentication data

* The System checks if the authentication data of the User are valid:
* Check if username exists
* Check if password matches username
* The System checks for the Sender Party if electronic signature is required based on CRED\_SIG\_REQUIRED and the signature is required

# System authenticates user

* The systems checks the electronic signature and the validation is successful
* The User is authenticated

# System checks the integrity of the XML message

| ID | Description |
| --- | --- |
| RULE264 | The system checks that the SOAP message BODY contains only one child element (e.g. *SubmitInboxRequest*) |
| RULE60 | The system checks that the operation XML wrapper element contains one and only one element (e.g. *InboxRequest)* |

# System checks if the authenticated User can be authorised to access the services

* The System extracts the unique Sender Party ID from the message envelope header (*Header.BusinessHeader.Sender.Identifier*) together with the Receiver Party ID
* The System assigns a Sender Party Agreement to the user based on the User identity and the unique Sender Party ID
* The System checks that for the requested service there is at least one interchange agreement between the Sender and the Receiver Party.
* At this point the User is granted permission to access the services
* **Use Case ends.**

# Subflows

# Alternative Flows

TBD

# Exceptional Flows

# E1: At step 2.1.4 “System checks authentication data”, the authentication data is incorrect

* The System notifies the User that the authentication data is incorrect by sending a 401 “Unauthorized” Client Error
* The Use Case continues at step “2.1.2 System asks User for authentication”

# E2: At step 2.1.4 “System checks authentication data”, the http authentication header is missing

* The System notifies the User that the http authentication header is incorrect by sending a 401 “Unauthorized” Client Error
* The Use Case continues at step “2.1.2 System asks User for authentication”

# E3: At step 2.1.6 “System checks the integrity of the XML message”, the message Body does not contain only one direct child element

* System submits a SOAP Fault [**5**] with the following description: “Undefined operation”
* This closes the https connection between the User and the system
* The Use Case Ends

# E4: At step 2.1.5 “System checks the integrity of the XML message”, the operation XML wrapper element does not contain one and only one element

* System submits a SOAP Fault [**7**]
* This closes the https connection between the User and the system
* The Use Case Ends

# E5: At step 2.1.4 “System checks authentication data”, and the digital signature is missing

* System submits a SOAP Fault [9] with description “Unauthorized Access”
* This closes the https connection between the User and the system
* The Use Case Ends

# E6: At step 2.1.4 “System checks authentication data”, and the certificate used for the digital signature is not trusted

* System submits a SOAP Fault [9] with description “Unauthorized Access”
* This closes the https connection between the User and the system
* The Use Case Ends

# E7: At step 2.1.4 “System checks authentication data”, and the validation of the digital signature fails

* System submits a SOAP Fault [9] with description “Unauthorized Access”
* This closes the https connection between the User and the system
* The Use Case Ends

# Special requirements

# Interface(s) with other Systems

* System submits a SOAP Fault [**7**]
* This closes the https connection between the User and the system
* The Use Case Ends

# Security Requirements

The reader should refer to chapter 1.1 Functional Features List of subtype "Security".

# Other Non Functional Features

Phase: Phase 1

*Non Functional: Usability* Maximum level of transparency, minimum effort and agreed level of security

# Constraints

Phase: Phase 1

*Constraint: Implementation* Open standards support

# Preconditions

# Precondition One

The User has to accept the SSL certificate of the server to be able to establish a secure connection.

# Precondition Two

The message size cannot exceed the maximum message size defined by the Application Server.

# Post conditions

# Post condition one

After the last step of the Use Case the User is validated in the System. The System can use the validated identity of the User to allow him to consume specific services or resources.

# Additional information

# Additional links

* The SOAP protocol specification can be found in [http://www.w3.org/TR/2000/NOTE-SOAP-20000508/http://www.w3.org/TR/2000/NOTE-SOAP-20000508/](http://www.w3.org/TR/2000/NOTE-SOAP-20000508/)
* A description of SOAP Faults can be found in <http://www.w3.org/TR/2000/NOTE-SOAP-20000508/#_Toc478383507>
* The HTTP protocol specification can be found in <http://www.w3.org/Protocols/rfc2616/rfc2616.html>

1. urn1 namespace is defined as xmlns:sbdh="http://www.unece.org/cefact/namespaces/StandardBusinessDocumentHeader" [↑](#footnote-ref-1)