ANNEX 6

SEF Tables

SIAR

Documentation on the Consolidated System of EU registries

UNFCCC SEF application

Version 1.2

Settings

Party:	Slovenia
ISO:	SI
Submission year:	2013
Reported year:	2012
Commitment period:	1
Completeness check:	YES
Consistency check:	YES
File locked:	YES
Lock timestamp:	8.4.2013 12:54
Submission version number:	2
Submission type:	Official

Party	Slovenia
Submission year	2013
Reported year	2012
Commitment period	1

Table 1. Total quantities of Kyoto Protocol units by account type at beginning of reported year

Account type	Unit type					
	AAUs	**ERUs**	**RMUs**	**CERs**	**tCERs**	**lCERs**
Party holding accounts	60777432	NO	NO	NO	NO	NO
Entity holding accounts	7878607	372163	NO	175237	NO	NO
Article 3.3/3.4 net source cancellation accounts	NO	NO	NO	NO		
Non-compliance cancellation accounts	NO	NO	NO	NO		
Other cancellation accounts	NO	NO	NO	NO	NO	NO
Retirement account	23221951	548673	NO	1286367	NO	NO
tCER replacement account for expiry	NO	NO	NO	NO	NO	
lCER replacement account for expiry	NO	NO	NO	NO		
lCER replacement account for reversal of storage	NO	NO	NO	NO		NO
lCER replacement account for non-submission of certification report	NO	NO	NO	NO		NO
Total	91877990	920836	NO	1461604	NO	NO

Party	Slovenia
Submission year	2013
Reported year	2012
Commitment period	1

Table 2 (a). Annual internal transactions

Transaction type	Additions						Subtractions					
	Unit type						Unit type					
	AAUs	ERUs	RMUs	CERs	tCERs	lCERs	AAUs	ERUs	RMUs	CERs	tCERs	lCERs
Article 6 issuance and conversion												
Party-verified projects		NO					NO		NO			
Independently verifed projects		NO					NO		NO			
Article 3.3 and 3.4 issuance or cancellation												
3.3 Afforestation and reforestation			NO				NO	NO	NO	NO		
3.3 Deforestation			NO				NO	NO	NO	NO		
3.4 Forest management			NO				NO	NO	NO	NO		
3.4 Cropland management			NO				NO	NO	NO	NO		
3.4 Grazing land management			NO				NO	NO	NO	NO		
3.4 Revegetation			NO				NO	NO	NO	NO		
Article 12 afforestation and reforestation												
Replacement of expired tCERs							NO	NO	NO	NO	NO	
Replacement of expired lCERs							NO	NO	NO	NO		
Replacement for reversal of storage							NO	NO	NO	NO		NO
Replacement for non-submission of certification report							NO	NO	NO	NO		NO
Other cancellation							NO	NO	NO	NO	NO	NO
Sub-total		NO	NO				NO	NO	NO	NO	NO	NO

Transaction type	Retirement					
	Unit type					
	AAUs	ERUs	RMUs	CERs	tCERs	lCERs
Retirement	7203813	631181	NO	165763	NO	NO

Party	Slovenia
Submission year	2013
Reported year	2012
Commitment period	1

Table 2 (b). Annual external transactions

	Additions						Subtractions					
	Unit type						Unit type					
	AAUs	ERUs	RMUs	CERs	tCERs	lCERs	AAUs	ERUs	RMUs	CERs	tCERs	lCERs
Transfers and acquisitions												
DE	30000	NO	NO	58200	NO	NO	4310824	5000	NO	24100	NO	NO
BG	NO	25874	NO	NO	NO	NO	25874	NO	NO	NO	NO	NO
NL	25000	120120	NO	NO	NO	NO	71000	13404	NO	55568	NO	NO
CH	NO	945707	NO	135300	NO	NO	NO	325000	NO	46000	NO	NO
GB	19880	714032	NO	298385	NO	NO	287469	315770	NO	264829	NO	NO
FR	NO	3824	NO	10000	NO	NO	58824	NO	NO	NO	NO	NO
SK	NO	NO	NO	NO	NO	NO	28000	NO	NO	29770	NO	NO
BE	10000	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
EU	NO	119731	NO	NO	NO	NO	NO	449545	NO	76531	NO	NO
ES	NO	NO	NO	NO	NO	NO	3840	NO	NO	NO	NO	NO
IT	NO	NO	NO	NO	NO	NO	NO	3937	NO	NO	NO	NO
PL	NO	NO	NO	NO	NO	NO	NO	14690	NO	NO	NO	NO
NZ	NO	NO	NO	NO	NO	NO	NO	300629	NO	NO	NO	NO
Sub-total	84880	1929288	NO	501885	NO	NO	4785831	1427975	NO	496798	NO	NO

Additional information

Independently verified ERUs								NO				

Table 2 (c). Total annual transactions

Total (Sum of tables 2a and 2b)	84880	1929288	NO	501885	NO	NO	4785831	1427975	NO	496798	NO	NO

Party	Slovenia
Submission year	2013
Reported year	2012
Commitment period	1

Table 3. Expiry, cancellation and replacement

Transaction or event type	Expiry, cancellation and requirement to replace		Replacement					
	Unit type		Unit type					
	tCERs	lCERs	AAUs	ERUs	RMUs	CERs	tCERs	lCERs
Temporary CERs (tCERS)								
Expired in retirement and replacement accounts	NO							
Replacement of expired tCERs			NO	NO	NO	NO	NO	
Expired in holding accounts	NO							
Cancellation of tCERs expired in holding accounts	NO							
Long-term CERs (lCERs)								
Expired in retirement and replacement accounts		NO						
Replacement of expired lCERs			NO	NO	NO	NO		
Expired in holding accounts		NO						
Cancellation of lCERs expired in holding accounts		NO						
Subject to replacement for reversal of storage		NO						
Replacement for reversal of storage			NO	NO	NO	NO		NO
Subject to replacement for non-submission of certification report		NO						
Replacement for non-submission of certification report			NO	NO	NO	NO		NO
Total			NO	NO	NO	NO	NO	NO

Party	Slovenia
Submission year	2013
Reported year	2012
Commitment period	1

Table 4. Total quantities of Kyoto Protocol units by account type at end of reported year

Account type	Unit type					
	AAUs	**ERUs**	**RMUs**	**CERs**	**tCERs**	**lCERs**
Party holding accounts	56751275	NO	NO	NO	NO	NO
Entity holding accounts	NO	242295	NO	14561	NO	NO
Article 3.3/3.4 net source cancellation accounts	NO	NO	NO	NO		
Non-compliance cancellation accounts	NO	NO	NO	NO		
Other cancellation accounts	NO	NO	NO	NO	NO	NO
Retirement account	30425764	1179854	NO	1452130	NO	NO
tCER replacement account for expiry	NO	NO	NO	NO	NO	
lCER replacement account for expiry	NO	NO	NO	NO		
lCER replacement account for reversal of storage	NO	NO	NO	NO		NO
lCER replacement account for non-submission of certification report	NO	NO	NO	NO		NO
Total	87177039	1422149	NO	1466691	NO	NO

Party	Slovenia
Submission year	2013
Reported year	2012
Commitment period	1

Table 5 (a). Summary information on additions and subtractions

	Additions						Subtractions					
	Unit type						Unit type					
Starting values	**AAUs**	**ERUs**	**RMUs**	**CERs**	**tCERs**	**lCERs**	**AAUs**	**ERUs**	**RMUs**	**CERs**	**tCERs**	**lCERs**
Issuance pursuant to Article 3.7 and 3.8	93628593											
Non-compliance cancellation							NO	NO	NO	NO		
Carry-over	NO	NO		NO								
Sub-total	93628593	NO		NO			NO	NO	NO	NO		
Annual transactions												
Year 0 (2007)	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Year 1 (2008)	5000	NO	NO	390468	NO	NO	205165	NO	NO	2734	NO	NO
Year 2 (2009)	90598	NO	NO	1017469	NO	NO	823132	NO	NO	200000	NO	NO
Year 3 (2010)	331407	315610	NO	607745	NO	NO	1025046	19000	NO	500833	NO	NO
Year 4 (2011)	1155971	873336	NO	966097	NO	NO	1280236	249110	NO	816608	NO	NO
Year 5 (2012)	84880	1929288	NO	501885	NO	NO	4785831	1427975	NO	496798	NO	NO
Year 6 (2013)	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Year 7 (2014)	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Year 8 (2015)	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Sub-total	1667856	3118234	NO	3483664	NO	NO	8119410	1696085	NO	2016973	NO	NO
Total	95296449	3118234	NO	3483664	NO	NO	8119410	1696085	NO	2016973	NO	NO

Table 5 (b). Summary information on replacement

	Requirement for replacement		Replacement					
	Unit type		Unit type					
	tCERs	**lCERs**	**AAUs**	**ERUs**	**RMUs**	**CERs**	**tCERs**	**lCERs**
Previous CPs			NO	NO	NO	NO	NO	NO
Year 1 (2008)		NO	NO	NO	NO	NO	NO	NO
Year 2 (2009)		NO	NO	NO	NO	NO	NO	NO
Year 3 (2010)		NO	NO	NO	NO	NO	NO	NO
Year 4 (2011)		NO	NO	NO	NO	NO	NO	NO
Year 5 (2012)	NO	NO	NO	NO	NO	NO	NO	NO
Year 6 (2013)	NO	NO	NO	NO	NO	NO	NO	NO
Year 7 (2014)	NO	NO	NO	NO	NO	NO	NO	NO
Year 8 (2015)	NO	NO	NO	NO	NO	NO	NO	NO
Total	NO	NO	NO	NO	NO	NO	NO	NO

Table 5 (c). Summary information on retirement

	Retirement					
	Unit type					
Year	**AAUs**	**ERUs**	**RMUs**	**CERs**	**tCERs**	**lCERs**
Year 1 (2008)	NO	NO	NO	NO	NO	NO
Year 2 (2009)	8062990	NO	NO	797115	NO	NO
Year 3 (2010)	7532582	169605	NO	367952	NO	NO
Year 4 (2011)	7626379	379068	NO	121300	NO	NO
Year 5 (2012)	7203813	631181	NO	165763	NO	NO
Year 6 (2013)	NO	NO	NO	NO	NO	NO
Year 7 (2014)	NO	NO	NO	NO	NO	NO
Year 8 (2015)	NO	NO	NO	NO	NO	NO
Total	30425764	1179854	NO	1452130	NO	NO

Party	Slovenia
Submission year	2013
Reported year	2012
Commitment period	1

Table 6 (a). Memo item: Corrective transactions relating to additions and subtractions

	Additions						Subtractions					
	Unit type						Unit type					
	AAUs	ERUs	RMUs	CERs	tCERs	lCERs	AAUs	ERUs	RMUs	CERs	tCERs	lCERs

Table 6 (b). Memo item: Corrective transactions relating to replacement

	Requirement for replacement		Replacement					
	Unit type		Unit type					
	tCERs	lCERs	AAUs	ERUs	RMUs	CERs	tCERs	lCERs

Table 6 (c). Memo item: Corrective transactions relating to retirement

	Retirement					
	Unit type					
	AAUs	ERUs	RMUs	CERs	tCERs	lCERs

No problems found!

SIAR Reports

R-2: List of discrepant transaction

DES Respond Code	Average naumber of occurences per transaction (X 100.000)		Transaction Number	Proposal Date Time	Transaction Type	Final State	Explanation	Units involved abbreviated		
	Reported Year	Prior to the Reported year						Serial Number	Unit Type	Quantity

No discrepant transaction for the reporting period, pursuant of 15/CMP.1 annex I.E paragraph 12.

R-3: List of CDM notifications

Notification Type	Notification Number	Notification Data Time	Tagred Number of Units	Number of Units Cancelle	Number of Units Replace	Difference		Explanation
						At target date	Post target date	

No CDM notifications were received by the National Registry during the reporting period, pursuant of 15/CMP.1 annex I.E paragraph 13 & 14.

R-4: List of non-replacements

List of non replacement for reversal of storage, non-submition of cerfitication report and impending expiry of ICER or tCER

Notification Type	Notification Number	Notification Data Time	Target Number of Units	Number of Units Cancelle	Number of Units Replace	Difference between tagred and cancellations or replacements		Explanation
						At target date	Post target date	

Non-replacement record for reversal of storage notification

Notification Number	Notification Type	Notification Data Time	Target Number of Units	Number of Units Cancelle	Number of Units Replace	Difference between tagred and cancellations or replacements		Explanation
						At target date	Post target date	

Units concerned		
Serial Number	Unit Type	Quantity

Non-replacement record for impending expiry of ICER or tCER

Notification Number	Notification Type	Notification Data Time	Target Number of Units	Number of Units Cancelle	Number of Units Replace	Difference between tagred and cancellations or replacements		Explanation
						At target date	Post target date	

Units concerned		
Serial Number	Unit Type	Quantity

Non-replacement record for non-submission of certification report

Notification Number	Notification Type	Notification Data Time	Target Number of Units	Number of Units Cancelle	Number of Units Replace	Difference between tagred and cancellations or replacements		Explanation
						At target date	Post target date	

Units concerned		
Serial Number	Unit Type	Quantity

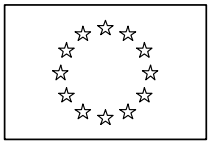
No non-replacements occurred during the reporting period,pursuant of 15/CMP.1 annex I.E paragraph 15.

R-5: List of individual units report layout

Serial Number	Unit Type	Quantity	Transaction Number

No invalid units to list for the reporting period, pursuant of 15/CMP.1 annex I.E paragraph 16

ETS LIMITED



EUROPEAN COMMISSION

DIRECTORATE-GENERAL
CLIMATE ACTION

EU Registry

Application Logging Plan

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: BU-5 - Tel. direct line +32 229-84052

Contact:
VELGHE Ronald, Telephone:84052, ronald.velghe@ec.europa.eu

1. TRANSACTION LOG

The requirements presented in section 7.1 of the **[DES]** are met by the tables presented in Figure 1-1:

- The table Transactions contains the general information of a transaction (identifier, transferring/acquiring registry/account type/account identifier, etc.) for each transaction either sent or received by a registry consolidated within the EU Registry.
- The table Transaction_Block contains the list of transaction block involved in each transactions
- The table Transaction_Status_History contains the history of the transaction statuses
- The table Transaction_Response contains the list of response codes returned for a transaction
- The table TXResponse_TXBlocks make the link between transaction blocks and returned response codes.

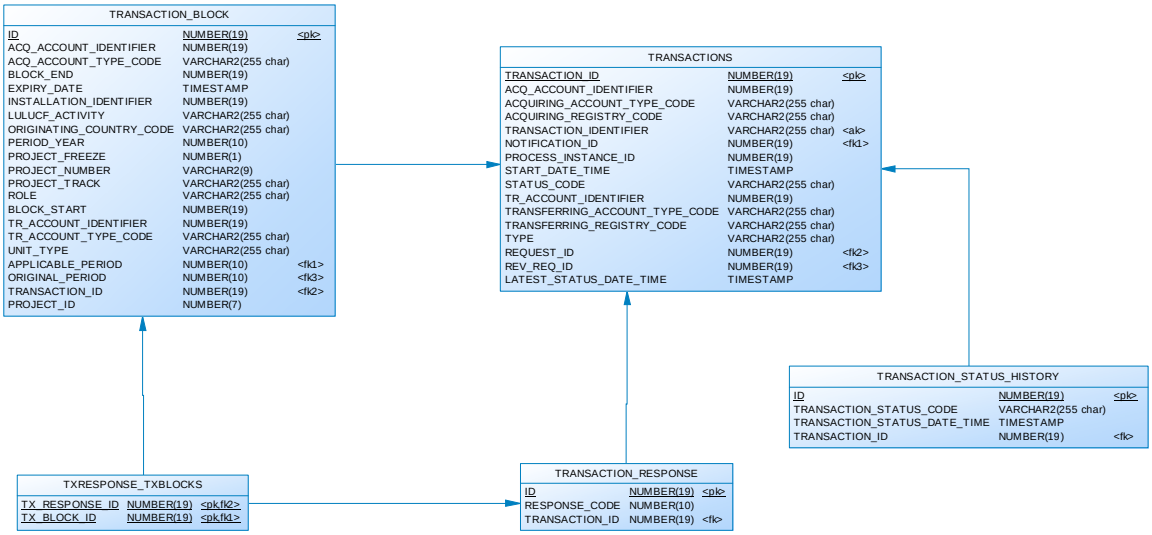


Figure 1-1: The tables related to the transaction logging

2. RECONCILIATION HISTORY LOG

The requirements presented in section 7.2 of the **[DES]** are met by the tables presented in Figure 2-1:

- The table Reconciliation presents each reconciliation executed for a registry consolidated within the EU Registry;
- The table Recon_Missing_Unit_Blocks contains for each reconciliation the list of blocks which were flagged as inconsistent by the ITL;
- The table Recon_Stage_History contains the status history of each reconciliation.

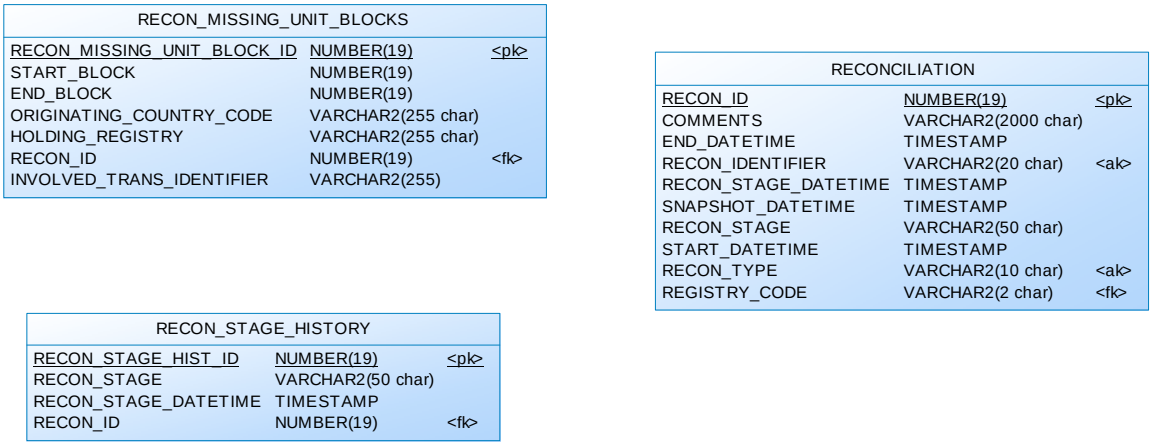


Figure 2-1: The tables related to the reconciliation logging

3. NOTIFICATION LOGGING

The requirements presented in section 7.3 of the **[DES]** are met by the tables presented in Figure 3-1:

- The table notification contains the list of each ITL notification sent to a registry consolidated within the EU registry;
- The table Notification_Unit_Blocks contains the list of unit block contained within an Impending Expiry Date notification.

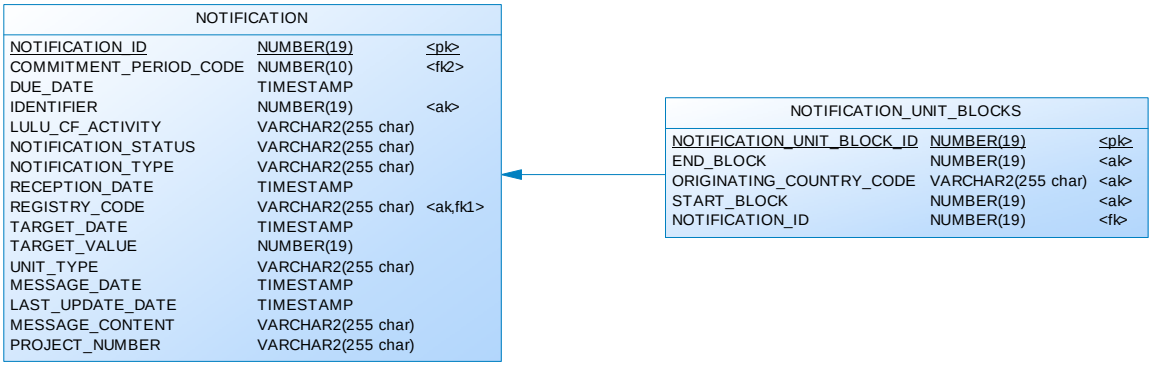


Figure 3-1: the tables related to the ITL notification logging

4. INTERNAL AUDIT LOG

The EU Registry generates log files named registry_XX.log where XX is the ISO 3166 country code of one of the registries consolidated within the EU Registry. Those log files are kept in the file system of the EU Registry server. There is such a log file for each of the consolidated registries. Each entry in those log files corresponds to an activity performed by a national user in the Web application of the EU Registry, each entry contains:

- Timestamp;
- Country code of the registry;
- Identifier of the server;
- Identifier of the user if available (some functionalities are available to anonymous users);
- Identifier of the activity;
- The IP address of the request;
- A description of the activity along with the values provided by the user.

This meets the requirements of the section 7.4 of the DES because the impacted table and fields can be deduced from the activity identifier (the same tables and fields are always impacted by the same activity). Furthermore, the sole user operations which can impact transactions and reconciliation processes are the creation, update, and deletion of unit blocks. In case of creation, the values of the unit block parameter are provided by the log entry; in case of update, the values before and after are provided; finally in case of deletion, the originating country code, unit serial start number, and unit serial end number are provided.

5. MESSAGE LOGGING

The received and sent WS requests and responses are recorded in dedicated xml files whose name format is a unique number for the day and registry suffixed by _REQ (for request) or _RES (for response). The archiving is organized by day and registry. The root of the message archive is the folder “message_archive” which is stored in the file system used by the EU Registry. This folder contains sub-folders for each registry whose name is the ISO 3166 country code of the registry. Each registry folder contains also 2 sub-folders: IN or OUT for storing separately the incoming and outcoming messages. Each of those folders contains a sub-folder per day whose name has the format YYYYMMDD (year, month, day). This folder contains a sub-folder for each server. And finally those folders contains a sub-folder whose name is a numeric, a new sub-folder is created once the current sub-folder exceed 1,000 messages. A short example of the file structure is presented below:

- Message_archive
  - GR
    - IN
      - 20111114
        - Server1
          - 000
            - 000061_REQ.xml
            - 000062_RES.xml
          - 001
        - Server2
      - 20111115
    - OUT
  - HR

The EU Registry has a table dedicated to the indexing of the received messages. This table is presented in Figure 5-1.

MESSAGE_LOG		
MESSAGE_LOG_ID	NUMBER(19)	<pk>
DATE_TIME	TIMESTAMP	
DELIVERY_STATUS	NUMBER(1)	
DIRECTION	VARCHAR2(3 char)	
MESSAGE_ID	VARCHAR2(50 char)	
MESSAGE_CONTENT	VARCHAR2(255 char)	
REGISTRY_CODE	VARCHAR2(2 char)	
REQUEST_LOCATION	VARCHAR2(255 char)	
RESPONSE_LOCATION	VARCHAR2(255 char)	
SERVER_NAME	VARCHAR2(50 char)	
WEBSERVICE_OPERATION	VARCHAR2(64 char)	

Figure 5-1: the table related to the logging of WS message

ETS LIMITED

EUROPEAN COMMISSION

DIRECTORATE-GENERAL
CLIMATE ACTION

EU REGISTRY

Change Management Procedure

Date: 15/11/2011

Version: 1.1

Authors:

Revised by:

Approved by:

Public:

Reference Number:

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: BU-5 - Tel. direct line +32 229-84052

ETS LIMITED

Document History

Version	Date	Comment	Modified Pages

Contact:
VELGHE Ronald, Telephone:84052, ronald.velghe@ec.europa.eu

Change Management Procedure

1 Introduction

Change management is the process of tracking change requests, confirming their validity, prioritising and authorizing (or rejecting/deferring) them. Following the acceptance of a change request, its development and implementation can commence.

2 Scope

Changes to the following elements shall be covered by this change management procedure:

- Data Exchange & Technical Specifications (DETS)
- Registry system interfaces to the users, the CITL and ITL infrastructure
- Functionality of the Union Registry
- Common operational procedures

Excluded from the scope of this change management procedure are:

- Changes to the Registry Regulation

3 Objectives

The objectives of this change management procedure are to:

- Ensure that all changes to in-scope components are effectively and efficiently recorded, evaluated, planned and managed.
- Clearly define the change management responsibilities and actions to be undertaken by the involved parties.
- Minimise disruption to the operations provided, reducing incidents and problems resulting from change.
- Improve ability to deal with resulting incidents and problems as details of the change will have been communicated in advance.
- Maximise visibility and communication of in-scope changes.

4 Roles

4.1 Originator

The Originator is the person or party that initially proposes a change. This might be a registry administrator of an EU Member State or an EEA country that participates in the EU ETS, the Union registry administrator or the CITL Administrator. The Originator has to ensure that a change is proposed with all the necessary and correct information.

4.2 Union registry change manager (URCM)

This role is responsible for managing the overall change management procedure and ensuring its effective implementations. The role of the URCM is taken over by the Union registry administrator.

The responsibilities of the URCM are:

- Chairing the CMB, facilitating consensus in decision making
- Ensuring that CMB reaches conclusion on proposed changes
- Ensuring that CMB decisions take account of required resources to implement changes in the Union registry
- Working with the Originator to ensure that all change requests contain all necessary information to evaluate a proposed change and reject invalid changes (e.g. out-of-scope of the procedure)
- Reviewing each change request, classifying it, coordinating impact assessments and proposing packages of changes to be considered together.
- Ensuring that change requests are responded to in a timely manner.
- Scheduling, preparing information for (including impact assessments), and arranging participation at the CMB for the changes to be discussed.
- Ensuring the correct implementation of the change procedure and recommend amendments to the procedure as necessary.

4.3 Service provider change manager

This role within the Union registry service provider organisation is responsible for working with the Union registry change manager to support the preparation and consideration of change requests in case of changes to the Union registry.

The responsibilities of the Service provider change manager are the following:

- Working with the URCM to ensure the completeness of change requests
- Working with the URCM to assess the impact of changes and propose solutions to change requests
- Implementing the change in the Union registry

4.4 Change management board (CMB)

This role is responsible for reviewing all change requests, impact assessments and proposed solutions in order to approve, defer or reject change requests. The specific responsibilities of the CMB are:

- Assess all change requests with regard to risk, impact and business benefit.

- Review and approve (or defer or reject) change requests taking into account required resources to implement changes to the Union Registry.
- Determine the priority of change requests and assign proposed changes to releases.

The CMB consists of the Union registry change manager and four registry administrators. After the URCM has issued a call for candidates, the EU Member States and EEA countries that participate in the EU ETS may propose registry administrators as candidates for the CMB. The CMB members will then be elected at the next meeting of the registry administrators. All Member States and EEA countries that participate in the EU ETS have one four votes that may be distributed in any portion to the candidates[1]. If they are not present at the registry administrators meeting they might delegate their voting rights to one of the other Member States or EEA countries that participate in the EU ETS. The four candidates with the highest number of votes are elected. If the result of the vote is not clear because more than one candidate has the same number of votes a run-off vote will take place between the candidates with the same number of votes.

In the beginning of every year after the completion of the first year of existence of the CMB two of the four seats of the CMB are up for reelection. Members of the CMB may serve in the CMB for a maximum of two consecutive years. However, there is an exception to this rule in case an insufficient number of new candidates are nominated for CMB membership.

5 Change Management Procedure

5.1 Submit change request

A change request might be submitted to the Union registry change manager (URCM) by an Originator, which may be might be a Registry Administrator of an EU Member State or an EEA country that participates in the EU ETS, the Union registry administrator or the CITL Administrator. Several of these parties may also submit a change request in cooperation. The number of parties that support a change request will be taken into consideration by the Change Management Board (CMB) when deciding upon the change request.

The Originator may subsequently seek to withdraw a change request by contacting the URCM.

5.2 Record change request

The Union registry change manger (URCM) records all valid change requests and allocates a unique change request number to the request. The URCM ensures that only justified change requests, with sufficient explanatory information, are accepted. A proposal that is not sufficiently elaborated will be referred back to the Originator for clarification or further information. The URCM maintains a list of all recorded change requests and their current status. This list is available through the Circa Website to all registry administrators.

[1] Four votes per Member State / EEA country are necessary because four positions are up for election. This mechanism allows Member States / EEA country to vote for the four candidates which should compose the CMB or distribute the votes freely between any candidates. If every Member State / EEA country has only one vote there is the risk that fewer than four candidates will receive all the votes.

The URCM may also rule that the proposed change is invalid because it lies, for example, outside the scope of this procedure or is in conflict with EU legislation such as the Registry Regulation (2216/2004 in its current version). The URCM has to report any change requests that are rejected at this level to the CMB for information.

5.3 Classify and prioritise change request

The Union registry change manager (URCM) classifies and prioritises the change request based on the criteria of expected impact, urgency and registry administrator support. See point 5. Classification and prioritisation of changes below.

5.4 Carry out impact assessment

The URCM requests an impact assessment from all affected parties that has to be carried out and submitted to the URCM within two weeks. The URCM assembles the impact assessments into one single document to be considered by the CMB. The impact assessment shall include an assessment of the consequences if the change is not implemented.

In case of changes to the Union registry an impact assessment carried out by the Union registry service provider is mandatory. In case of changes to the Union registry or common operational procedures other affected parties might carry out an impact assessment, e.g. registry administrators, to assess the impact on their national procedures, workload, etc.

The impact assessment for changes that are classified as urgent is fast-tracked. Such impact assessment is undertaken by the URCM. Where circumstances permit, key affected parties are directly consulted and may also provide impact assessment.

In case it is unclear to the URCM whether an impact assessment is required at this early stage the URCM may also proceed directly with step 4.5 and leave the decision on the impact assessment to the CMB.

5.5 Compile and submit change request to change management board (CMB)

The URCM compiles the completed impact assessments and prepares packages of information. The URCM submits all change requests together with the packages of information to the CMB for review. If no impact assessments have been carried out, the URCM only submits the change requests to the CMB.

The CMB may decide that only changes of a certain classification or prioritisation are submitted to it for review and other changes are decided upon by the URCM directly. The CMB may decide on criteria for this classification or prioritisation.

5.6 CMB review

The URCM coordinates the activities of the CMB to review and approve change requests. The URCM convenes CMB meetings, prepares and distributes materials in advance and chairs the CMB meetings. The CMB has to convene a minimum of six times a year. In case an urgent change request is recorded by the URCM, a CMB meeting has to be convened within the next two weeks. CMB meetings may also take place virtually, e.g. via tele- or videoconference.

The information on the classification and priorisation of the change request that has been prepared by the URCM defines the order in which change requests are considered by the CMB and serve as additional information on the change.

Based on the submitted materials the CMB may:

- Approve change requests
- Defer change requests pending further information
- Request further information including impact assessments
- Decide whether the standard timeframe for an impact assessment being two weeks is extended
- Reject change request
- Confirm dates for the release of the change
- Review progress on the release of changes

The CMB approves change requests on the basis of consensus or rejects or defers the request. Where a change request is dividable, the CMB may approve, reject or defer a change request in parts or may approve a change request in stages.

The URCM prepares minutes of the CMB meetings and provides them to all registry administrators via the Circa Website.

5.7 Authorise change and release date

Subject to approval of the CMB the URCM authorizes changes and the dates for their release. The URCM communicates authorization of a change to the Service provider change manager and other affected parties in order that they may commence implementation work.

In cases in which the CMB defers or rejects a change request, the URCM communicates this to affected parties and the Originator of the change request.

5.8 Revise specification (e.g. DETS)

The CMB may decide that after having agreed upon a change request other specifications, procedures or change requests need to be adapted. The revision of the specifications is coordinated by the URCM prior to the release of a change. A change to the DETS has to be authorised by the Climate Change Committee. Changes to common operational procedures have to be authorised by the working group on the specific procedure. Revisions of other types of specifications may be approved by the URCM. The URCM may seek CMB approval of such revised specifications in order to confirm that they are consistent with the change request originally authorised.

5.9 Release management (in case of software change)

5.10 Please consult [Version Change Management]Close change request

If all authorized work on a change has been completed successfully the URCM closes the change requests after authorisation by the CMB.

6 Classification and prioritisation of changes

The classification of changes helps the URCM and the CMB to prioritise the review and the implementation of change requests. Changes that are major, urgent and are supported by many registry administrators are prioritised over minor changes with low urgency that are supported by few registry administrators.

6.1 Impact Classification

- Major
  Changes requiring significant implementation effort by the Union registry and national registry administrators and involving large risks to their development and operation. Changes have typically not been undertaken before and the impacts are unknown at the point of raising the change request.
- Minor
  Changes involving well-established solutions where the change is predictable from previous experience and the impacts are controllable and well understood.

6.2 Urgency classification

- Low
  The Change is not necessary to the proper operation of the Union registry. In many cases the Change is:
  - A minor enhancement
  - A defect with an existing and effective workaround

  The Release of the Change may be delayed until after the next scheduled Release with no significant consequences.
- High
  The Change is expected to significantly improve the operation of the Union registry. In many cases the change is:
  - A defect with an unsatisfactory or no workaround which prevents or restricts the operation of one or more functions
  - A substantial enhancement
  - A legal requirement

  The Release of the change must be included in the next scheduled Release.

6.3 Registry administrator support

Information on how many registry administrators from different EU Member States of EEA countries participating in the EU ETS support the change. This information is derived either from the number of Member States or EEA countries that submitted a change request in cooperation and/or comments by registry administrators as a result of the impact assessment.

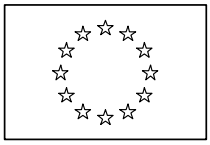
7 Target timeframe

The progress of an individual change request through the procedure depends on factors such as scale, complexity and clarity of information. The following target timeframe is proposed:

Procedural step	**Target timeframe**
Submission of change request	Any time
Record CR	1 week after submission
Submission impact assessments	2 weeks after classification. The CMB may extend this period if the change

	request is submitted first to the CMB.
Submission of CR package to CMB	2 weeks after impact assessment
Authorization of change and release date	1 week after CMB meeting
Revision of relevant specifications	4-8 weeks after CMB meeting
Authorisation of DETS change by CCC	At the next CCC
Closure of CR	1 week after the CMB meeting where the closure of the request is authorised

ETS LIMITED



EUROPEAN COMMISSION

DIRECTORATE-GENERAL
CLIMATE ACTION

EU Registry

Disaster Recovery Plan

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: BU-5 - Tel. direct line +32 229-84052

Contact:
VELGHE Ronald, Telephone:84052, ronald.velghe@ec.europa.eu

1. ROLES AND RESPONSABILITIES

Please refer to **[Roles and Responsibilities]**.

2. DISASTER RECOVERY STRATEGY

Please see the Crisis Management procedure in **[Joint Business Continuity Plan]**

3. MINIMUM HARDWARE AND SOFTWARE REQUIREMENTS

The EU Registry is a Java EE applications which must be deployed on a Weblogic 11 cluster composed of at least 2 nodes. Its operations require also an Oracle 11 database and a load balancer. The machines hosting the Weblogic nodes and the database should be Solaris servers. Finally the sytem would need a file system with at least 500 GB of free space.

4. PROCEDURE FOR BACKUP ROLLBACK

In the case where the disaster has resulted in a data corruption in the main site then the following procedure must be applied for restoring the data; it is assumed that the ITL and EUTL service desk have already been informed of the disaster and have temporarily suspended the right of the EU-ETS member states to submit requests:

1. Request the backup and restore team to restore the latest backup and provide the timestamp of this restored backup
2. Request the ITL Service Desk to provide a list of all the transactions involving a member state which have been updated between the backup timestamp and now. The status history and the transaction block must be provided along
3. Review the provided list in order to find transactions missing in the restored database or which have a different status. For each found transaction:
    a. If the transaction was not yet completed in the ITL then cancel it
    b. If the transaction is completed in the ITL then manually apply it in the EU Registry's database
4. Request the EUTL of all the processes (ETS transactions, account creation or update, NAP update, etc.)
5. If a review of those process records shows unknown process records or processes in a different status then manually apply the changes in the EU Registry's database.
6. Perform a successful ITL reconciliation with each member state (if a reconciliation fails, perform the required correction and restart a new one until successful completion)
7. Perform a sucessful ETS reconciliation (if the reconciliation fails, perform the required correction and restart a new one unti successful completion).
8. Inform the ITL and EUTL service desks that the EU Registry is ready to go back in operation

The executant of this procedure is the Central administrator.

5. LOCATIONS OF SITES

The production EU Registry is hosted at the DIGIT Luxembourg primary site while the DRP EU Registry is hosted at the DIGIT Luxembourg Backup site. Both sites meet the minimum operating requirements which have been presented in section 3. Copies of the crisis management documents are available at those sites through the EC's Intranet, furthermore the officials are

required to have copies of those documents on their personal computers. The actual address of those sites is a sensitive information and cannot be communicated.

6. ROLES AND RESPONSABILITIES AT DRP SITE

6.1. IT Team leader backup, storage, and infrastructure

This role is ensured by a main responsible and a backup. The responsabilities are the supervisions of the infrastructure and the procedures set in place by the European Commission in order to ensure the data storage, the backup and the disaster recovery of the applications hosted by the Commission.

6.2. IT system engineer

This role is ensured by a team of people. Their responsibility is the maintenance and support of the infrastructure set in place by the European Commission in order to ensure the data storage, the backup and the disaster recovery of the applications hosted by the Commission.

7. DATA REPLICATION TOOL

The data of the EU Registry can be separated in 2 parts:

- The database
- The file system which contains all the log files generated by the application

The file system is automatically replicated between the main site and the DRP site by EMC MirrorView while the database is replicated by Oracle Streams.

8. RECOVERABLE DATA

The EU Registry is considered as a critical system and thus as presented in page 10 of **[Service Level Agreement]:**

- Disasters which do not impact the integrity of data do not result in a loss of more than 1 hour of data
- Disasters which impact the integrity of data do no result in a loss of more than 1 day of data

In case of data loss, part of the database loss could be compensated by reconciling with the databases of the ITL and of the EUTL.

9. COMMUNICATION MECHANISMS

When a crisis affecting the EU Registry has been declared as described in section 3 of **[Joint Business Continuity Plan]**, the Central Administrator who is part of the crisis management team contacts by e-mail or phone each of the registry administrators to inform him or her of the crisis. Whenever a significant change of the crisis situation occurs, the Central Administrator will once again communicate it to the registry administrators. The registry administrators are free to decide whether or not they transmit the information to their users and the communication mean for doing so.

The registry administrators must provide their contact information to the Central Administrator and inform him of any change in their team composition.

10. RETURN TIME TO OPERATIONS

The EU Registry is a critical application for the trading of emission units; consequently the crisis management will strive to have the system back in operation within 48 hours as presented in page 10 of **[Service Level Agreement].**

ETS LIMITED

EUROPEAN COMMISSION

DIRECTORATE-GENERAL
CLIMATE ACTION

EU Registry

ITL Manual Interventions

Date:	15/11/2011
Version:	1.1
Authors:	
Revised by:	
Approved by:	
Public:	
Reference Number:	

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: BU-5 - Tel. direct line +32 229-84052

Document History

Version	Date	Comment	Modified Pages
0.1	27/07/2011	First draft of the document	

Contact:
VELGHE Ronald, Telephone:84052, ronald.velghe@ec.europa.eu

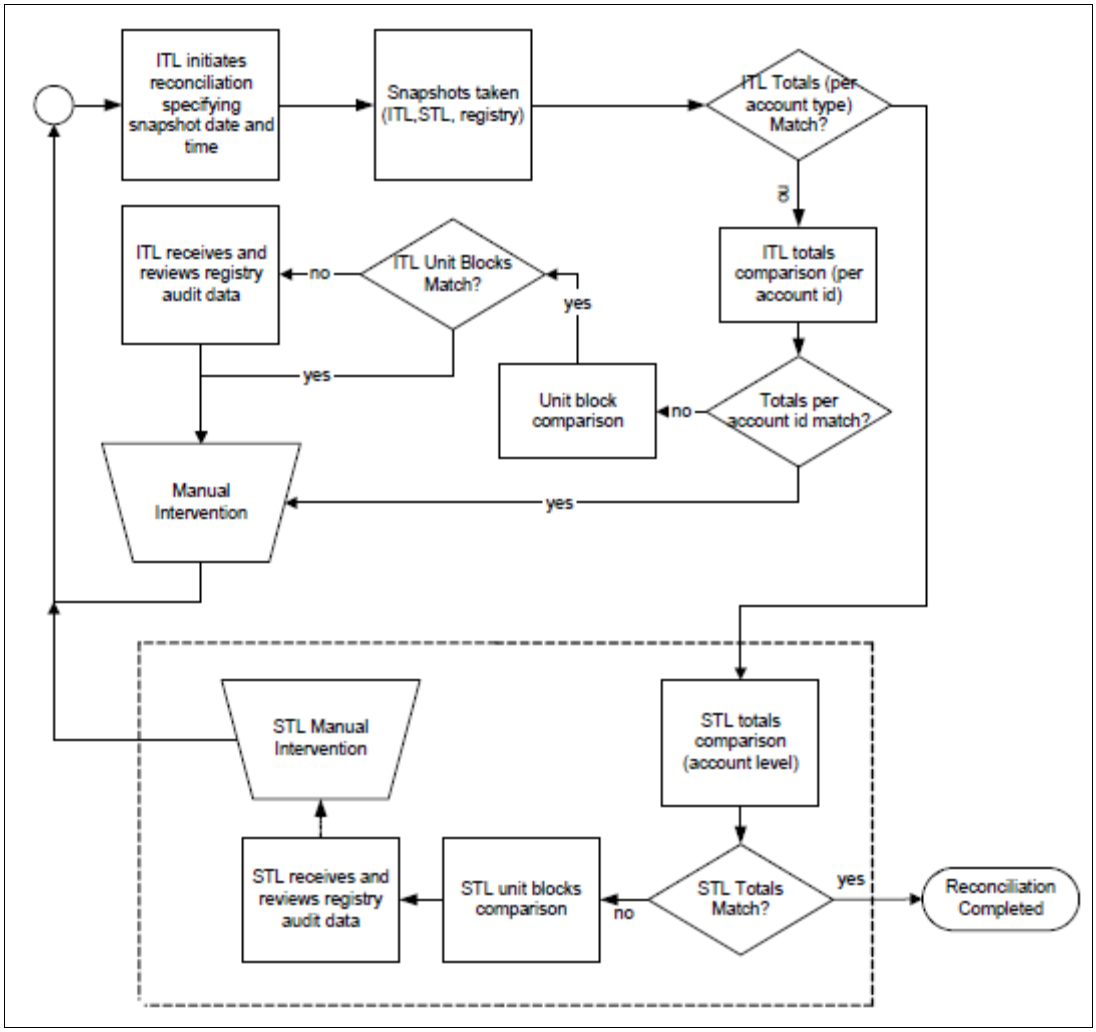
1. ROLES AND RESPONSABILITIES

Please refer to **[Roles and Responsibilities]**.

2. ITL RECONCILIATION PROCEDURE

The ITL Reconciliation presented in **[Reconciliation Procedure]** is a semi-automated process which enables to detect inconsistencies between the databases of the various registries, the ITL, and the STL (EUTL) with regards to unit holdings. The transactions transferring ETS allowances are not forwarded to the ITL and as a consequence, the ITL is un-aware of allowances holdings. Therefore the ITL procedure only covers the holdings of Kyoto units. The reconciliation of ETS holdings is handled by another process called "ETS Reconciliation Procedure" which is out of this document' scope.

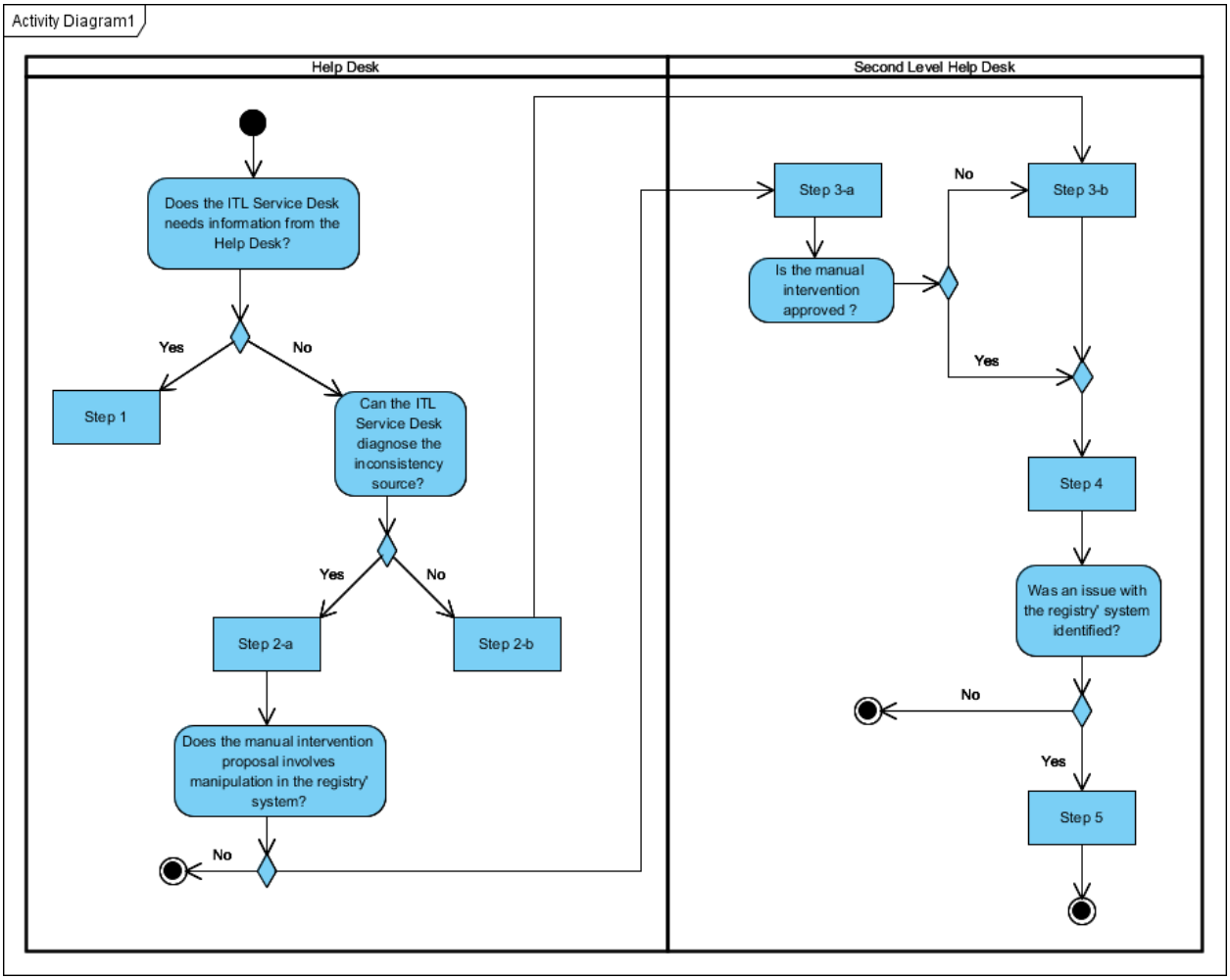
As presented in figure 2-1, the reconciliation procedure has 2 stages. Stage 1 is the comparison of the unit holdings between the registry and the ITL, stage 2 is the comparison of the unit holdings between the STL (EUTL) and the registry. An inconsistency in stage 1 is solved by an ITL Manual Intervention (Manual Intervention is the picture below), an inconsistency in stage is solved by a STL Manual Intervention.



2-1: Extract from Reconciliation Procedure: the process of an ITL Reconciliation

3. ITL MANUAL INTERVENTION

Please note that most inconsistencies found in stage 1 ITL Reconciliations are expected to be due to transactions which are stuck in a non-final state and are therefore finalized in the ITL but not in the registry (or reversely). Most of the ITL Manual Interventions should consist in the ITL Service Desk re-emitting a lost transaction message or manually advancing the state of a transaction.



3-1: The flow process of a manual intervention

3.1. Step 1 Research Transactions (optional)

This step is optional as the ITL Service Desk may be able to directly determine the origin of an inconsistency only with the data available in the ITL.

The ITL Service Desk contacts the Help Desk in order to obtain the current status of a list of transactions. The Help Desk must retrieve the current status of those transactions and provide the information to the ITL Service Desk

3.2. Step 2-a Manual Intervention Approval

The ITL Service Desk has successfully diagnosed the cause of the inconsistency and provides to the Help Desk a manual intervention proposal as presented in section 3 of **[Reconciliation Procedure]**. The Help Desk reviews the manual intervention proposal and notifies the ITL Service Desk of its approval it if it doesn't involve manipulation in the registry' system. Otherwise it forwards the manual intervention proposal to the Second Level Helpdesk.

If the manual intervention is approved then the ITL Service Desk performs the manual intervention, closes the reconciliation, and schedules a new one.

3.3. Steb 2-b Escalate the Issue

If the ITL Service Desk fails to diagnose the problem then the Help Desk escalates the issue to the Second Level Help Desk.

3.4. Step 3-a Manual Intervention Approval

The Second Level Help Desk reviews the manual intervention proposal provided by the ITL Service Desk in collaboration with the Registry Administrator. If the proposal is approved then the Second Level Help Desk implements it (step 4), if not then it starts its own investigation (step 3-b)

3.5. Step 3-b Investigation

The Second Level Help Desk in conjunction witht ITL Service Desk, EC Central Help Desk, and Registry Administrator investigates the source of the inconsistency and submits a manual intervention proposal to all involved parties. This step ends once the proposal has been accepted by all parties. If the manual intervention proposal requires a manipulation in the registry's database then the Second Level Help Desk implements it (Step 4)

3.6. Step 4 Implement Manual Intervention

The Second Level Help Desk implements the manual intervention proposal which has either been agreed on by all the concerned parties in the previous steps. Once it is done, it informs the ITL Service Desk which will close the reconciliation and schedule a new one.

3.7. Step 5 Preventing Further Occurences

If the investigation concluded that the origin of the inconsistency was an issue in the registry's system then the Second Level Help Desk must issue a change request as presented in **[Change Management Procedure]** for addressing the problem and submits it to the registry administrator for approval. Upon approval the Registry Administrator provides the change request to the maintenance team for an emergency release.

While the change request is being processed, the Second Level Help Desk must attempt to propose a workaround for preventing further occurrence of the inconsistency. If no workaround can be proposed then the registry must suspend its activities until a new version addressing the change request is released.

4. STL MANUAL INTERVENTION

Please note that the transaction message flow has been designed in such a way that transactions are not completed in the related registry-(ies) as long it has not been completed in the STL. Consequently, it is not possible that an inconsistency found in stage 2 to be due to a pending transaction. Consequently, the STL Manual Intervention follows the same process flow than the ITL Manual Intervention (see figure 3-1) but it starts directly in step 3-b.

ETS LIMITED

EUROPEAN COMMISSION

DIRECTORATE-GENERAL
CLIMATE ACTION

EU Registry

Operational Plan

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: BU-5 - Tel. direct line +32 229-84052

Contact:
VELGHE Ronald, Telephone:84052, ronald.velghe@ec.europa.eu

1. ROLES AND RESPONSABILITIES

Please refer to **[Roles and Responsibilities]**.

2. OPERATIONAL LOGS AND RECORD KEEPING

The EU Registry logs the following data in its database:

- Transaction along with their change history
- Reconciliations (ITL and ETS) along with their change history,
- ITL Notifications along with their change history,
- WS Message sent and received,
- Account-related processes (creation, update, closure, etc.) history,
- User-related processes (sign-up, approval, revocation, etc.) history,
- NAP-related processes history,
- JI projects history,
- ITL Notifications history.

The EU Registry stores the following data:

- User information,
- Account details and holdings,
- NAP and compliance of each member states,
- JI Projects

Please note that registry administrator do not have a direct access to the database and can only access those data trough the Web interface of the EU Registry. This Web interface has been designed and tested in order to prevent a registry administrator to access data which is not related to his own registry. Possibly, the registry administrator could be given in the future an access to the database through an Oracle Virtual Private Database access which will prevent them from accessing data related to another registry.

The EU Registry also keeps log files for each registry, those log files are kept in folders dedicated to each registry. Those log files contain the following:

- Copy of the Web Service messages received and sent;
- Activity of the users.

3. ONGOING PERFORMANCE EVALUATIONS AND ASSESSMENTS

The continued availability of the EU Registry is verified by using the MORE tool (see **[MORE]**). This tool is used to check at regular intervals that a few key pages of the EU Registry's Web interface are displayed within an acceptable interval.

A continuous security assessment is performed by an automated parsing of the user activity which detects suspicious patterns.

4. DATA MANAGEMENT

4.1. Data capture

Most of the data of the EU Registry is encoded through the Web interface of the EU Registry. This interface has several built-in business checks which ensure that the data is consistent. Furthermore the data encoded by users must always be reviewed by a second person before being recorded; for user details and account details, the review is performed by a registry administrator; for transaction details, the review is performed by a second user.

Another source of data are messages received from the EUTL and the ITL, those messages are also submitted to a series of business checks in order to ensure that they are consistent before they are recorded and processed.

Finally the operational data, the basic data necessary for the operation of the EU Registry (unit type codes, transaction type codes, etc.), is recorded by the execution of SQL scripts by the Database Administrator. Those scripts have been provided by the Maintenance Team and reviewed by the Central Administrator before being applied.

4.2. Data retrieval and usage

The availability of data depends on the person trying to access it:

- Anonymous users: they have access to the data presented in the public Web pages of the EU Registry;
- Users: they have access to their personal data and to the details of the accounts they are related to;
- Registry Administrator: they have access to all data which is relevant to their own registry;
- Central Administrator: they have access to all the EU Registry data.

4.3. Data storage

All the business-relevant data (transaction history, account holding, user details, etc.) is stored in the EU Registry's database. Besides that, the user activity trail and copies of the messages sent and received are stored in log files.

4.4. Data ownership

It is is considered that each Registry Administrator is the owner of his registry data. Consequently the Registry Administrators are also responsible of the correctness and consistency of their registry's data.

4.5. Data migration

The EU Registry is replacing the individual registry system of each member of the EU-ETS. Therefore the European Commision has produced the following document: **[Migration Plan]** for defining a format for the export of the registries data and their import into the EU Registry.

5. MODERNISATION AND TECHNOLOGY ASSESSMENT STRATEGY

The EU Registry is mainly based on the Weblogic application server and the Oracle database. The European Commission has teams dedicated to reviewing patches and upgrades of those technologies. Those teams advise whether it is recommended or necessary to upgrade those

techonologies by the mean of a change request. The European Commission has also asset management procedures for replacing and updating the hardware and software used for the hosting and monitoring of the EU Registry as those techonologies become obsolete and are replaced by new ones.

A part of the Maintenance Team mission is to evaluate on a regular basis whether it is necessary to update or replace the libraries used for the implementation of the EU Registry. When they identify such a need, this team prepares a change request and submit it.

6. TECHNICAL SUPPORT PLAN

The European Commission has procedures for hiring personel with IT skills and training them in order to maintain a pool of IT talents for supporting the applications used by the European Commission. Some of the IT skills which are maintained are:

- Database technologies (Oracle, SQL Server, MySQL, etc.),
- Middleware technologies (Weblogic, JBoss, WebSphere, etc.),
- Network technologies (WAN, LAN),
- Internet technologies (SSL, TLS, http, etc.),
- Desktop technologies,
- Data storage technologies,
- Server technologies (Unix servers, Wintel server).

7. INCIDENT MANAGEMENT

Please refer to **[Incident Management Procedure]**.

8. CHANGE MANAGEMENT

Please refer to **[Change Management Procedure**] for the handling of change requests and **[Version Change Management]** for the change of software version

9. LICENCES & PATCHES

Each software product used by the European Commission is assigned to a product manager. The role of the product manager is to ensure that the product licencing is ongoing and valid. Furthermore a product manager must oversee the delivery of patches and oversee their application in the various systems which use the software product.

Patches with a low criticality are applied during the scheduled downtime of the applications. Patches with a high criticality are applied ASAP by scheduling urgently a downtime of the application.

10. NAME AND VERSION OF THE APPLICATION

The name of the software product used by the EU Registry is the CSEUR: Consolidated System of European Registries. The fist version to be used in production will be the version 3.1

11. SERVICE PROVIDERS

Trasys is in charge of:

- Maintenance of the CSEUR,
- 2nd level service desk available from 7 to 19h (CET) during working days, 24h/7 during periods identified as critical.

Iris is in charge of 1st level service desk available aslo from 7 to 19h (CET) during working days, 24h/7 during periods identified as critical.

12. OPERATING HOURS

The EU Registry should be available anytime but as presented in page 11 of **[Service Level Agreement]**, the normal working hours range from 08:00 to 19:00 on working days.

Normal system maintenance should not last more than 4 hours and be scheduled outside the working hours.

Major system maintnenace should not last more than 12 hours and be scheduled outside of working hours

Maintenance of the computer room should take maximum 6 days per year and also be scheduled outside of working hours.

13. ENVIRONMENTS USED

The production EU Registry will work on the Production Environment.

2 test environments also exist:

- Acceptance (linked to the Registry environment of the ITL)
- Test (linked to the Developer environment of the ITL)

14. THE HOSTED REGISTRIES

The following registries are hosted within the EU Registry:

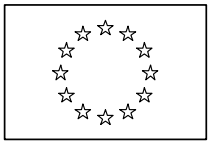
1. Austria
2. Belgium
3. Bulgary
4. Cyprus (not a KP Registry)
5. Czech Republic
6. Denmark
7. Estonia
8. European Commission
9. Finland
10. France
11. Germany
12. Greece

13. Hungary
14. Iceland
15. Ireland
16. Italy
17. Latvia
18. Lietchenstein
19. Lithuania
20. Luxembourg
21. Malta (not a KP registry)
22. Netherlands
23. Norway
24. Poland
25. Portugal
26. Romania
27. Slovenia
28. Slovakia
29. Spain
30. Sweden
31. United Kingdom

15. HELPDESK SUPPORT

The registry administrator will receive helpdesk support through IRIS (1st level) and Trasys (2nd level). The registry administrators are in charge of providing helpdesk support to their end users.

ETS LIMITED



EUROPEAN COMMISSION

DIRECTORATE-GENERAL
CLIMATE ACTION

EU REGISTRY

Roles and Responsibilities

Date:	27/07/2011
Version:	0.01
Authors:	Sébastien Gamby
Revised by:	
Approved by:	
Public:	
Reference Number:	

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: BU-5 - Tel. direct line +32 229-84052

Document History

Version	Date	Comment	Modified Pages
0.1	27/07/2011	First draft of the document	

Contact:
VELGHE Ronald, Telephone:84052, ronald.velghe@ec.europa.eu

1. ROLES AND RESPONSABILITIES

The following roles and responsabilities have been defined for the development, maintenance, and operation of the EU REGISTRY with respects to **[EC 1]**

1.1. European Commission

The European Commission is the owner of the EU REGISTRY and is responsible for the day-to-day operation, the hosting, and the administration to the EU REGISTRY. The roles within the European Commision are depicted below.

1.1.1. Central Administrator

The Central Administrator is responsible for the following:

- Ensure the compliance of the EU REGISTRY's operations with the EU legislation and the UNFCCC rules.
- Request and approve changes to the EU REGISTRY's IT system. The Central Administrator must verify that the modified system continues to comply with the EC legislations and the UNFCCC rules.
- Liaise with the service providers to ensure performance of contracts.
- Advice staff in the Commission and the member states on the applicable provisions in the EU legislation and UNFCCC rules.
- Answer any queries the member states (MS) or general public may have on policy in compliance with the public service obligation on the European Commission.
- Receive queries from the public and member states concerning legal and emission trade issues. The Central Administrator answers questions about procedures and regulations regarding emission transactions.
- Inform the member states and the service desks when the EU REGISTRY is unavailable or experiencing
- Liaise with the UN on any pertinent issues related to CR
- Ensure that the database content is consistent and is in line with the EU legislation and the KP rules.

Please note that the Central Administrator is actually a team of people. There is always a member available to assume the role at any time.

1.1.2. DG Clima LSO

The Director General of DG Clima has appointed a Local Security Officer (LSO) who is responsible for the global security environment. The LSO monitors the correct implementation of the DG Clima internal security rules, as laid down in Commission provisions on security **[Internal Rules of Procedure]** and **[IRP Update]**. The LSO is a key element in the overall general security structure of the DG. The LSO promotes security awareness within DG Clima, acts as a first port of call on general security issues and reinforces the effectiveness of the DG Clima's general internal security controls.

1.1.3. DG Clima LISO

The Director General of DG Clima has also appointed a Local Informatics Security Officer (LISO) within DG Clima who has special responsibility for information security and with

particular expertise in the IT aspects The DG Clima LISO is responsible for advising DG Clima on information security policy matters, reviews and recommends any necessary changes to this plan or to measures adopted under it. The DG Clima LISO is responsible for the dissemination of this plan within DG Clima, and of all measures & controls taken under it, to all staff to whom it applies and for raising and maintaining security awareness and good security practice throughout the organisation.

The DG Clima LISO has responsibility for liaison on information security matters with the Commission's Security Directorate, for advising on current and future Commission information security guidelines, the issue of specific DG ENV security plans, guidelines and procedures that complement this plan and the communication on information security trends and developments.

The DG Clima LISO also advises the EU REGISTRY Manager on issues arising from the implementation of this plan and has responsibility for auditing compliance. The DG ENV LISO is responsible for investigating information security incidents and for reporting security threats or risks.

1.1.4. DIGIT Local Informatics Security Officers

The Local Informatics Security Officer (LISO) is responsible for the global security environment and has special responsibility for information security and with particular expertise in the IT aspects.

1.1.5. Database Administrator

The Database Administrator is responsible for the support and maintenance of the, databases and transaction log files of the CR and coordinates change request (THM) concerning the hosting of the CR.

1.1.6. Network Administrator

The Network Administrator is responsible for the support and maintenance of the infrastructure on which the EU REGISTRY is operated. This includes networks, storage and back-up machines and their software as well as hardware components. The Network Administrator is also responsible for all issues concerning telecommunications.

1.1.7. EC Central Helpdesk

DG DIGIT Central Help Desk (operated by DIGIT/A1) receives questions and incidents notifications from DG ENV and the Maintenance team leader (MSP) concerning software, network and infrastructural issues and dispatch these calls and requests to the appropriate operational groups.

1.2. Contractor

1.2.1. Organisation of Maintenance team leader

The Maintenance team leader maintains the CR application. These activities will be performed by the following key staff:

1.2.1.1. Maintenance Team Leader

The Maintenance Team Leader has the overall responsibility to manage the infrastructure and the maintenance team.

1.2.1.2. Maintenance Team Member

These programmers will be responsible for production of the updated code that meets the release specifications. The programmers will also execute regression tests on their adaptations.

1.2.1.3. Application Manager

The incumbent for this role within the maintenance team leader has the following responsibilities:

- Deals with queries from MS and the Commission. They act as the primary contact person for the MS concerning technical problems that occur within the System. They therefore often function as a coordinator for solving problems between parties
- Sets up a reconciliation run between each MS Registry and CITL; each MS Registry's reconciliation is done at a specific time each evening for that MS
- Checks the reconciliation processes of all the connected MS to the CR have run properly and corrects where necessary. The ITL will also perform reconciliations, but this is outside the scope of this document
- Approves changes to the IT system, subject to the authorization of the Transaction Log Manager. They should ensure that the change meets DES requirements e.g. backward compatibility
- If there are any problems, the Application Manager contacts MS (copying Kyoto first level Help Desk on that message) and works with the Transaction Log Manager to solve any issues, acting as a coordinator between the MS and the Kyoto first level Help Desk
- Can implement changes authorised by the Transaction Log Manager to data on system by performing a manual intervention
- Gives support to MS
- Can delete a registry or launch a registry from the application, with the authorisation of the Central Administrator
- Monitors the quality of the service through involvement in test activities and day-to-day service monitoring
- Is informed by Maintenance team leader of any impending upgrade or version and can give input as to the timing of the implementation, prior to any new version being put into production
- If a MS registry is unavailable, the Application Manager publishes this information on the CR public website and sends information to support the TL Manager. The TL Manager then sends a CIRCA message to all Registry Managers informing them.

1.2.2. Organisation of CR Help Desk Services

The Help Desk Service Provider will provide the first-level Help Desk for the CR applications. This party deals with queries on the CR application from MS and the Commission.

These activities will be performed by the organisation described below:

1.2.2.1. Help Desk Team Leader

The Help Desk Team Leader will be a senior person who has the overall responsibility to manage the Help Desk team and to organize the service in the most effective and professional way.

1.2.2.2. Help Desk Team Member

The Help Desk Teammemberwill be responsible for the calls and the follow up from creation until closure; listen to the users and to translate their problems towards a technical team. The team member will have an understanding of the CR systems. They will have the expertise to write procedures and documentation for the problems and solutions discovered.

1.2.2.3. Second Level Help Desk Manager

This role will be responsible for the management of the second level help desk. They will ensure that all queries received are logged and properly dealt with. This role will have a dedicated functional email address and direct dial number.

1.3. Member states

The EU REGISTRY consolidates the registries of all the EU-ETS member states.

1.3.1. Registry administrator

The Registry administrator is in charge of the users and processes which concern only its registry. They have the following responsabilities:

- Ensure that the data entered by the users of their registry is correct,
- Handle failed reconciliation between their registry data and the EUTL or ITL,
- Encode data necessary for the operation of their registry such as NAP information, AAU issuance limits, etc.

1.3.2. Users

The end users of the EU REGISTRY are account representatives; that is persons which are related to a specific account. Their responsabilities are:

- Provide their personal information upon registration,
- Inform of any update of their personal information,
- Provide information for the account details,
- Encode transactions for their account,
- Respect the EU legislation and the KP rules.

A user must have submitted its personal data and been approved by a Registry Administrator in order to obtain access to a registry hosted by the EU REGISTRY. A user who wants to have access to several registries must obtain the approval of each Registry Administrator.

1.3.3. Anonymous Users

The EU REGISTRY has public Web pages which can be accessed by anyone without any authentication or access approval being necessary. Those users have no responsabilities.

ETS LIMITED

EUROPEAN COMMISSION

DIRECTORATE-GENERAL
CLIMATE ACTION

EU Registry

Security Plan

Contact:
VELGHE Ronald, Telephone:84052, ronald.velghe@ec.europa.eu

1. ROLES AND RESPONSABILITIES

Please refer to **[Roles and Responsibilities]**.

2. SERVER SECURITY

The Weblogic servers and Oracle Database servers are protected by login and password. Remote access requires a VPN connection whose authentication scheme relies on the use of personal tokens. The servers are also confined within a logic network domain which is firewalled and protected against viruses.

The EU Registry has been classified as "EU CONFIDENTIAL". Therefore the physical machines hosting the EU Registry servers are stored in a class II security area accordingly with the provisions presented in section 18.3 of **[Internal Rules of Procedure]**. The access to the machines is reserved to officials who have undergone the screening procedure presented in section 20 of **[Internal Rules of Procedure]**. Other persons can access the machines when necessary but only if they are accompanied by trusted personel who have undergone the screening procedure.

3. USER AUTHENTICATION

The EU Registry being a system of the European Commission, the authentication of its users is handled by the ECAS (European Commission Authentication Service). The basic authentication under ECAS relies on username/password, the password must be at least 10 characters long and the chose characters must belong to at least 3 of the following character groups:

- Upper Case: A to Z
- Lower Case: a to z
- Numeric: 0 to 9
- Special Characters: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

Examples: qlpDhXaGh2, IOphEZAqL8, EQ9HwOEtnv

The passwords expire 180 days after their creation or update. A notice is sent by e-mail to the user 5 days before the expiration. If a user enters five consecutive times a wrong password then this user is blocked for 15 minutes during which he cannot try to log in.

For sensible applications such as the EU Registry, ECAS also implements a second level of authentication which relies on the use of a non-encrypted SMS containing a one-use and short-lived (5minutes) code sent to the mobile phone of the user. Finally please note that there is an under work project named Stork. The aim of this project is to enable ECAS to use electronic identity card as a second level of authentication. Assuming that this project is a success and is widely adopted by member states then the EU Registry might use in the future electronic identity card as a second level of authentication. It is foreseen that the support of electronic identity card should be effective within 5 years.

This authentication mechanism applies to all users including the member state administrators.

4. USER AUTHORISATION

As the user authentication is handled by ECAS, an external agent, and as the registry administrators want to control who can access the non-public Web pages of the EU Registry dedicated to their member state; an ECAS login is not sufficient for getting access to the non-public pages of the EU Registry such as the Account List, the Transaction List, etc.

A user who wants to be granted access to a member state's registry hosted by the EU Registry must first fill an online form for providing personal information along with scans from its identity

papers. Upon review, the registry administrator decides whether or not the access request is granted. Please note that a registry administrator granting access to his registry to a specific user does not affect the access rights of the same user for the other registries. Therefore a user who wants access to several registries hosted by the EU Registry must repeat the procedure for each registry. Once the user request has been accepted and that he becomes representative of at least one account in the registry, he receives offline (conventional mail, phone, etc.) an enrolment key that he must enter online in order to be given access to the registry.

For administrators, the processus is the same except that the enrolment key is directly sent to them upon approval of their registration request. They do not need to be nominated representative of an account.

5. TRADING PLATFORMS AUTHENTICATION

The trading platform systems send requests to the EU Registry for initating transaction on behalf on their clients, querying the balance of a managed account, etc. The authentication of the trading platform will be performed by verifying that their requests are digitally signed and that the used digital certificate is valid.

6. SESSION SECURITY

The EU Registry communicates over the Internet with the following systems and persons:

- Users and administrators;
- ITL;
- Trading platforms systems.

Please note that the EUTL is not listed above because it is hosted alongside the EU Registry in the EC Luxembourg primary site. Therefore communications between the two systems are confined within the secured network of the EC and do not require encryption.

The communication between the EU Registry and the ITL are encrypted accordingly with the provisions presented in section 3.3 of [**DES**]. The communications between the EU Registry and the users, administrator, and trading platforms use TLS (Transport Layer Security) connections in order to ensure the encryption of communication. The TLS protocol is an evolution of the SSL protocol which is more secure. The used version of TLS is 1.0 or above.

7. AUDITING

The log files generated by the Weblogic servers, Oracle Database servers, operating systems are stored and backed up. No cleanup of those files is currently foreseen. An automated monitoring of those log files has been set in order to detect intrusion attempts and othe suspect activities.

The EU Registry also generates application logs fore each member state which contain an entry each time a user executes an action in the EU Registry Web interface or when a trading platform sends a request. An action can be the initation of a transfer, the consultation of an account, etc. The log entry will provide the unique identifier of the person or system at the origin of the action, the IP address used, and details of the action (e.g. for the creation of account it would be the account identifier, its type, etc.). Finally, the EU Registry for each incoming or outgoing Web service message, the EU Registry generates a disctinct log file containing a copy of the message and writes an entry in a database table for recording general details of the message (sender, receiver, WS operation, etc) and the name of the generated log file.

8. DEPRECATED AND REVOKED USERS

A user who is no longer associated to any account or a user suspected or convinced of having broken European or national rules related to the use of the EU Registry will be un-enrolled by an administrator meaning that the EU Registry will refuse subsequent login requests from this user. No user accounts will ever be deleted. A user who has been un-enrolled can be re-enrolled but with a different user account which will be linked to the same ECAS account. The same ECAS account cannot be related to more than one open user account at any time.

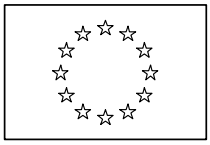
9. NON-REPUDIATION

The EU Registry requires the user to sign important operation such as the initiation of transaction, the modification to administrators, and the modifications to the unit block holdings. This signature is handled by ECAS and it consists in sending to the user a non-encrypted SMS containing a summary of the operation along with a short-lived (5minutes) one-off code. The user reviews the SMS and if the content matches the expected details, then the user enters the code hereby signing the operation.

10. PRIVATE KEY PROTECTION POLICY

The private keys are stored in password-protected JKS keystores which are stored in the file system of the EU Registry server and therefore replicated in the DRP site and backed up. Only the Central Administrator knows the passwords of the keystores and of the contained keys (each private key has its own password).

ETS LIMITED



EUROPEAN COMMISSION

DIRECTORATE-GENERAL
CLIMATE ACTION

EU Registry

Time Validation Plan

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: BU-5 - Tel. direct line +32 229-84052

Contact:
VELGHE Ronald, Telephone:84052, ronald.velghe@ec.europa.eu

1. TIME SYNCHRONISATION

The time synchronisation service used by the EU Registry is the one set in place by the European Commission for serving all its computers. This service is actually a NTP (Network Time Protocol) version 4.2 and it uses a clock strata architecture.

The first clock stratum is the atomic clock hosted in Frankfurt (Germany), this clock broadcast the current time over radio waves accordingly with the DFC77 protocol.

The second clock stratum is a set of UNIX servers which synchronize their time by receiving the radio signal emitted by the stratum 1 clock. Each building of the European Commision has 2 of those servers, which also synchronise their time between the two of them with the NTP protocol.

The third clock stratum is composed of a set of NTP distribution servers which synchronise their time between themselves and the whole set of second clock stratum servers with NTP. Those servers are split into 2 pools of machines identified by pool1.ntp.cc.cec.eu.int and pool2.ntp.cc.cec.eu.int. Each pool's machines are hosted in disctinct buildings from the machines of the other pool.

The fourth clock stratum is composed of the standard machines used to host the applications of the European Commission such as the EU Registry. They synchronise their time through NTP with two stratum 3 server, one from each pool, which guarantees that each machine synchronise with stratum 3 servers located in different buildings.

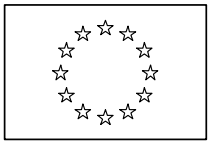
2. SCHEDULE AND DRIFT TOLERANCE

Each machine of the fourth clock stratum refreshes its time every 5 minutes. The time drift tolerated for a stratum 4 machine is 3.2×10^{-5} second. The NTP daemon are automatically monitored and if a time drift superior to the tolerated value is experienced, an alert will be dispatched to a unit dedicated to the resolution of time synchronisation issues which will investigate it.

3. OUT OF CONTROL TIME VALIDATION

If the process of time validation is no longer working properly, this is considered as a catastrophic failure of the host environment. The crisis management procedure described in **[Joint Business Continuity Plan]** is triggered and the crisis management team should decide to immediately switch off all the impacted application including the EU registry. If the DRP site is un-affected then it will take over the operations. The normal operations will not be resumed until the issue witht the time validation is solved.

ETS LIMITED



EUROPEAN COMMISSION

DIRECTORATE-GENERAL
CLIMATE ACTION

EU Registry

Version Change Management

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: BU-5 - Tel. direct line +32 229-84052

Contact:
VELGHE Ronald, Telephone:84052, ronald.velghe@ec.europa.eu

1. ROLES AND RESPONSABILITIES

Please refer to **[Roles and Responsibilites]**.

2. VERSION CHANGE PROCEDURE

This procedure describes how the EU Registry evolves from a version to another. It must not be confused with the Change Management Procedure which describes how a single change request is handled. Both procedures are interconnected because new versions are meant to address one or more change requests.

This procedure is followed for all release of the EU Registry. The normal flow of the procedure is presented below.

1. Definition of the scope and schedule of the release
2. Implementation of the release
3. Delivery and acceptance of the release.
4. Deployment of the release

In the case where issues occur during one of the steps, then the procedure is re-started from step 1. The following sub-sections depict each of the procedure steps.

2.1. Definition of the scope and schedule of the release

During the development of the EU Registry, the number of releases, their content, and their schedule is agreed upon by the central administrator and the maintenance team leader at the beginning of the development project. During the maintenance of the EU Registry, the decision to organise a new release can be prompted by 2 reasons:

- Normal release: The implementation of new functionalities, the improvement of existing functionalities, and the resolution of non-critical bugs,
- Emergency release: the resolution of critical bugs.

A bug is considered critical if it prevents the users to perform important operations or if it results in a corruption of the business data stored in the EU Registry. The scope of a release will be expressed in the form of a set of JIRA issues capturing the various requirements of the European Commission with regards to the new release. The normal releases will be scheduled in order to allow sufficient time for a correct implementation and testing of the EU Registry's new version. Emergency release will be scheduled in order to have the required bug fixes implemented, tested, and deployed as fast as possible. The scope and schedule of the releases are agreed upon by the central administrator and the maintenance team leader.

2.2. Implementation of the release

Once the scope and schedule of the release is decided, the maintenance team members develop the new version of the EU Registry with respects to **[Software Development Plan]** and perform the factory acceptance as described in the **[Project Test Plan]**.

2.3. Delivery and acceptance of the release

The procedure for the delivery and acceptance is presented in section 2.3 of **[Acceptance Test Plan]**. A typical delivery will contain the following:

- Source code (optional),
- J2EE archives (EARs, WARs, and JARs) built from the source code,
- Installation guide,
- Release notes,

- FAT report,
- Set of Weblogic scripts for updating the Weblogic domains,
- Set of SQL scripts for modifying the database schema,
- Set of SQL scripts for uploading data into the database.

2.4. Deployment of the release

At this point, the new EU Registry's release has been delivered, tested and accepted by European Commission. The following procedure is then followed for deploying the provided release in the Production environment.

1. Schedule of the deployment: for normal releases, the central manager chooses a date where the usage of the EU Registry is expected to be low in order to limit the disruption of the service for the users. For emergency releases, the central manager will choose the closest possible date.
2. Notification of the stakeholders: with regards to the strategy presented in section 8, the central administrator notifies all the stakeholders about the the impending update of the EU Registry and the consequent disruption of service.
3. Stopping the EU Registry: the network administrator stops all the Weblogic applications which compose the EU Registry.
4. Failover preparation: in order to cope with a failure during the deployment, the network administrator takes a snapshot of the Weblogic domains; while the database administrator takes a snapshot of the database.
5. Installation of the release: with respects to the instructions provided in the delivery's installation guide, the DIGIT network administrator updates the Weblogic domains with the provided Weblogic scripts and installs the provided J2EE archives. The DIGIT database administrator uses the delivered SQL scripts for updating the database schema and uploading new data.
6. Re-start of the EU Registry and evaluation: the network administrator re-starts all the Weblogic applications which compose the EU Registry. Once it is done, the network administrator verifies through the Weblogic consoles and the other available monitoring tools that the EU Registry is running correctly.

If issues are found during the installation of the new release or its evaluation; then the network administrator will restore the Weblogic domains with the previously taken snapshots. The database administrator will do the same but for the database.

3. TESTING ENVIRONMENTS

The DG Clima is using 2 test environments named respectively TEST and ACC (acceptance). Both test environments have the following environments:

- A load balancer,
- An access to ECAS,
- A Weblogic 11 cluster, each server contains all the J2EE archives contained in a release,
- An access to an Oracle 11 database,
- An access to an EUTL test instance,

- An access to an ITL test instance, the TEST environment is connected to the Developer Test environment of UNFCCC and the ACC environment is connected to the Registry Test environment of UNFCCC.

Those environments are kept up and running permanently and there are no plans to take them down in the future. Furthermore those environments are part of the test cycles organised by the UNFCCC, see **[Registry Test Cycle]**.

4. DATA MANAGEMENT DURING RELEASE

4.1. Database upgrade

As stated above, a new release delivery can contain a set of SQL script which modifies the structure of the EU Registry's database and possibly introduces new operational data (basic data required for the operation of the EU Registry such as account type code enumeration). The review and test of those scripts is performed by the maintenance team during the factory tests and by the Central Administrator during the acceptance tests in order to ensure that no business data will be corrupted or lost because of those scripts.

4.2. Migration

The EU Registry is a consolidated registry which will host the registry of each ETS-Member states. Therefore the European Commission has devised a migration procedure (see **[Migration Plan]**) for ensuring the safe transfer of data from the deprecated registry system towards the EU Registry. This procedure would be re-sued if other registries join the EU Registry later on.

5. SOFTWARE BUILD AND VERSION CONTROL

As presented in section 6.2 of **[Software Development Plan]**, the EU Registry's deliverables are built thanks to Maven and the version changes of the source code are handled by Subversion.

6. DOCUMENTATION CONTROL

Please refer to section 2.1 of **[Acceptance Plan].**

Please note that a short summary to the track change is provided in each Word document.

7. NAMING CONVENTION

Each release will be identified by 2 numbers presented in this format: x.y. The first number is the major version number; the second one is the minor version number. A new version is considered as major if it brings new functionalities which represent a significant evolution of the system; otherwise it is considered as minor version.

8. NOTIFICATION STRATEGY

When a new version is about to come in Production, at least 5 working days before the deployment date, the Central Administrator will prepare an e-mail as following:

- Subject: Deployment of CSEUR version XX (where XX is the new version number)
- Content:

- The schedule of the deployment,
- the list of all the new features, improvements, and bug fixes addressed by the new version

- Recipients: the list of registry administrators, the ITL Service Desk, any other relevant STL Service Desk

The Registry Administrators are expected to inform their national users by the means they will see fit.