



UNFCCC ITL Administrator

Standard Independent Assessment Report Reporting Requirements and Guidance for Registries

Reference	IAR Procedure		
Security classification:	RSA Forum		
Version number:	v4.5	State:	Approved
Prepared by:	Neil Peerman, Carla Valle, Jean-Francois Halleux, UNFCCC, Chris Collins, Bryan Eckstein	Date:	07/12/2010
Reviewed by:	Mike Elhaddad	Date:	07/12/2010
Approved by:	Vitaly Matsarski	Date:	07/12/2010

Circulation list

Name/Role	Organization	Info/Action
RSA Forum	Registry System Administrators	Information

Document change record

Version	Date	Description	Affected sections
v2.3	04/11/2008	Feedback from third SIAR WG meeting and review comments included; fixed headers and footers and appendices; formatted.	All
v2.4	07/11/2008	Aligned the report on discrepancies with the ITL report to ease comparison, should it be needed. Clarified the requirement to report on CDM notifications Clarification of format to use when reporting	Report R-2, Report R-3, 1.1
v2.5	13/11/2008	Approved	All
v2.6	01/12/2008	Final	All
v2.7	04/03/2009	Final - spelling corrections	All
v2.8	30/06/2009	Merge of Requirements and Guidance notes	All
v2.9	27/07/2009	Updates following review with Secretariat	All
v2.10	27/08/2009	Added language in introduction, rationalized language, improved organization and formatting	All
v4.0	24/09/2009	Updated to correspond with other SIAR documents	All
v4.1	12/11/2009	Incorporating feedback from SIAR Working Group	Section 3.2
V4.3	20/01/2010	Updated for version consistency	All
v4.4	30/09/2010	Initial revisions following 2010 SIAR process to improve clarity	Section 3.2, Appendix 6, Appendix 7

V4.5	07/12/2010	Removed Response Code 3005	Table on P.16
------	------------	----------------------------	---------------

Table of Contents

1.0 Introduction.....	4
2.0 Annual Submission Report Structure.....	4
3.0 Detailed Reporting Guidance	4
3.1 Chapter 12: Information on Accounting of the Kyoto Protocol Units	4
3.1.1 Format for NIR Submission	5
3.1.2 File Format to Use When Submitting the Reports.....	7
3.2 Chapter 14: Information on Changes in National Registry	8
3.2.1 Format for NIR Submission	8
Appendix 1 – Report R-1: Standard Electronic Format (SEF).....	14
Appendix 2 – Report R-2: List of Discrepant Transactions	15
Appendix 3 – Report R-3: List of CDM Notifications	21
Appendix 4 – Report R-4: List of Non-replacements	23
Appendix 5 – Report R-5: List of Invalid Units	26
Appendix 6 – Further Detailed Information about Reporting Changes to National Registry	27
Appendix 7 – Readiness Documentation Reporting Guidelines	29

1.0 Introduction

This document describes the format of information to be provided by Parties as part of the annual submission in order to facilitate their assessment in the Standard Independent Assessment Report (SIAR) process and is a supplement to the guidance document titled "Annotated outline of the National Inventory Report including reporting elements under the Kyoto Protocol" available at:

http://unfccc.int/files/national_reports/annex_i_ghg_inventories/reporting_requirements/application/pdf/annotated_nir_outline.pdf

See the document "Common Operational Procedure: Independent Assessment Report (IAR) Procedure" (file IAR Procedure v4.0.pdf) for additional information on the SIAR process.

This document provides further guidance on the content that should be provided under "Chapter 12: Information on accounting of Kyoto Units" and "Chapter 14: Information on changes in national registry" and Annex 6 in the outline referenced above and referred to in the remainder of this document as the National Inventory Report (NIR).

2.0 Annual Submission Report Structure

In order to facilitate the Expert Review Team (ERT) assessment of a national registry, this guidance proposes a common reporting structure for information about Parties' national registries that is aligned with the requirements of the relevant decisions of the Conference of the Parties serving as the meeting of the Parties to the Kyoto Protocol (COP/MOP).

It is suggested that Parties report on information related to the national registry, which is part of the Party's annual submission, using the structure defined in the following sections.

3.0 Detailed Reporting Guidance

The following sections provide a description of the content to be included under each of the chapters presented for organizing the NIR. The same structure is mirrored by the ITL Administrator in the corresponding SIAR in response to the annual submission by the Party.

3.1 Chapter 12: Information on Accounting of the Kyoto Protocol Units

The following tables should be used as the basis for Chapter 12: Information on accounting of Kyoto units as referred to in the NIR outline. The following reports are described in this document and correspond to the requirements of decisions 14/CMP.1 and 15/CMP.1:

Report	Reference to Decision
R-1: Standard electronic format (SEF)	Decision 15/CMP.1, paragraph 11
R-2: List of discrepant transactions	Decision 15/CMP.1, paragraph 12
R-3: List of CDM notifications	Decision 15/CMP.1, paragraph 13 Decision 15/CMP.1, paragraph 14
R-4: List of non-replacements	Decision 15/CMP.1, paragraph 15
R-5: List of invalid units	Decision 15/CMP.1, paragraph 16

Detailed requirements for each report are provided in the first 5 appendixes to this document.

3.1.1 Format for NIR Submission

Guidance on specific items to be included in the Party's submission is provided below in the right hand column; the Party may wish to use a similar table structure in Chapter 12 of the NIR submission, replacing the right hand column with Party provided content.

Annual Submission Item	Reporting Guidance
<p>15/CMP.1 annex I.E paragraph 11: Standard electronic format (SEF)</p>	<p>A reference to Party's report in the standard electronic format (SEF) containing the information required in paragraph 11 of the annex to decision 15/CMP.1 and adhering to the guidelines of the SEF may be included in the NIR as Chapter 12.2 "Summary of information reported in the SEF tables" and the SEF report contents may be reproduced in annex 6 of the NIR. Suggested text for the NIR: "The Standard Electronic Format report for 20YY has been submitted to the UNFCCC Secretariat electronically and the contents of the report can also be found in annex 6 of this document."</p> <p>This SEF report is referenced as report R-1 in this document. See Appendix 1 for more details relating to the SEF report.</p> <p><i>Or</i></p> <p>A clear statement that the Party has not transferred or acquired Kyoto Protocol units prior to or during the reported year. Suggested text for the NIR: "A SEF Report has not been submitted to the UNFCCC Secretariat as the national registry has not transferred or acquired Kyoto Protocol units during or prior to 20YY."</p>
<p>15/CMP.1 annex I.E paragraph 12: List of discrepant transactions</p>	<p>A reference to Party's report of discrepant transactions (as report R-2 and, where applicable, report R-5) may be included in the NIR as Chapter 12.3 "Discrepancies and notifications" and report R-2 may be reproduced in annex 6 of the NIR. See Appendix 2 for requirements for report R-2 and Appendix 5 for report R-5.</p> <p><i>Or</i></p> <p>If no discrepancies occurred, a clear statement indicating no discrepant transaction for the reporting period, pursuant of 15/CMP.1 annex I.E paragraph 12. Suggested text for the NIR submission if no discrepancies occurred, "No discrepant transactions occurred in 20YY."</p>
<p>15/CMP.1 annex I.E paragraph 13 & 14: List of CDM notifications</p>	<p>A reference to Party's report of CDM notifications (as report R-3) may be included in the NIR as Chapter 12.3 "Discrepancies and notifications" and report R-3 may be reproduced in annex 6. See Appendix 3 for requirements for report R-3.</p> <p><i>Or</i></p> <p>If no CDM notifications occurred, a clear statement indicating that no CDM notifications were received by the National Registry during the reporting period. Suggested text for the NIR submission if no CDM notifications occurred, "No CDM notifications occurred in 20YY."</p>
<p>15/CMP.1 annex I.E paragraph 15:</p>	<p>A reference to Party's report of the list of non-replacements (as report R-4) may be included in the NIR as Chapter 12.3</p>

Annual Submission Item	Reporting Guidance
List of non-replacements	<p>"Discrepancies and notifications" and report R-4 may be reproduced in annex 6. See Appendix 4 for requirements for report R-4.</p> <p><i>Or</i></p> <p>If no non-replacements occurred, a clear statement indicating that no non-replacements occurred during the reporting period. Suggested text for the NIR submission if no non-replacements occurred, "No non-replacements occurred in 20YY".</p>
<p>15/CMP.1 annex I.E paragraph 16: List of invalid units</p>	<p>A reference to Party's report of the list of invalid units (as report R-5) may be included in the NIR as Chapter 12.3 "Discrepancies and notifications" and report R-5 may be reproduced in annex 6. See Appendix 5 for requirements for report R-5.</p> <p><i>Or</i></p> <p>If no invalid units occurred, a clear statement indicating no invalid units to list for the reporting period. Suggested text for the NIR submission if no invalid units occurred, "No invalid units exist as at 31 December 20YY".</p>
<p>15/CMP.1 annex I.E paragraph 17 Actions and changes to address discrepancies</p>	<p>A description of the detailed actions taken to correct any problem that caused a discrepancy to occur, any changes to the National Registry to prevent a discrepancy from reoccurring, or the resolution of any previously identified questions of implementation pertaining to transactions may be included in the NIR as Chapter 12.3 "Discrepancies and notifications" and the details included in annex 6.</p> <p>The details of the change and the documented results of the change should be submitted in accordance with the requirements for NIR Chapter 14: Information on Changes in National Registry described in Section 3.2 of this document.</p> <p><i>Or</i></p> <p>If no changes were made, a clear statement indicating no actions were taken or changes made to address discrepancies. Suggested text for the NIR submission if no actions were taken or changes made, "No actions were taken or changes made to address discrepancies for the period under review".</p>
<p>15/CMP.1 annex I.E Publicly accessible information</p>	<p>A URL for the Party's webpage containing publicly available information may be included in the NIR as Chapter 12.4 "Publicly accessible information." If information is deemed confidential, a discussion of the why the information is confidential (including the relevant reference to national and international legislation, if applicable) should be provided with specific reference to paragraphs 44-48 (Section E) in the annex to decision 13/CMP.1. See the separate guidance document on public information as required under section E of the annex to 13/CMP.1 for more information: "SIAR Publicly Available Information Reporting Guidance for National Registries."</p>
<p>15/CMP.1 annex I.E paragraph 18 CPR Calculation</p>	<p>A report of the calculation of the commitment period reserve, in accordance with the annex to decision 18/CP.7, should be included in the NIR as Chapter 12.5 "Calculation of the commitment period reserve (CPR)."</p> <p>Note that it is not sufficient to state that the CPR calculation</p>

Annual Submission Item	Reporting Guidance
	has not changed since the last submission: the detail of the calculation should be repeated in each NIR.

3.1.2 File Format to Use When Submitting the Reports

In addition to the report specific requirements in the first five appendixes, the following file formats should be used by Parties reporting under the SIAR process:

- Report R-1 (SEF) shall be submitted in the format established by the SEF specifications (currently, as an MS Excel application).
- Report R-2 to R-5 shall be submitted in one Excel file, with four sheets named respectively "R2", "R3", "R4" and "R5". The requirements for the reports are included in the annexes.
- The Excel file shall be compatible with Microsoft Excel 2003 and shall be named as such:

SIAR Reports [Reported Year]-[Party ISO 3166 3 letters Code] v[Major Version].[Minor Version].xls

For example, the Danish reports for 2009, first major version shall be named:

SIAR Reports 2009-DK v1.0.xls

3.2 Chapter 14: Information on Changes in National Registry

In all the following submission items, a Party must clearly describe the change in Chapter 14 and reference and attach the required documentation to support the assessment of the change in annex 6 to the NIR. **In case of no change, a Party must state clearly that no change occurred against the submission item during the reporting period.** To be clear, every reporting item in Section 3.2.1 should be associated with an explicit statement of “change” or “no change” (see below for suggested text). See appendix 6 of this document for additional guidance on what is considered a change and the baseline for reporting changes.

The following table should be used as the basis for Chapter 14: Information on Changes in National Registry as referred to in the NIR outline.

3.2.1 Format for NIR Submission

Guidance on specific items to be included in the Party’s submission is provided below in the right hand column; the Party may wish to use a similar table structure in Chapter 14 of the NIR submission, replacing the right hand column with Party provided content.

Reporting Item	Reporting Guidance
15/CMP.1 annex II.E paragraph 32.(a) Change of name or contact	State the change in name or contact information of the registry administrator designated by the Party. <i>Or</i> If no change occurred , indicate no change in this submission. Suggested text for the NIR submission if no change occurred, “No change in the name or contact information of the registry administrator occurred during the reported period”.
15/CMP.1 annex II.E paragraph 32.(b) Change of cooperation arrangement	State the change in the set of Parties with which the Party cooperates by maintaining national registries in a consolidated system (if any). A change to the cooperation arrangement would be considered a significant change: attach in annex 6 documents such as test plans, test reports, update to the registry readiness documentation to demonstrate the correct functioning of the registry after the consolidation / deconsolidation. <i>Or</i> If no change occurred , indicate no change in this submission. Suggested text for the NIR submission if no change occurred, “No change of cooperation arrangement occurred during the reported period”.

Reporting Item	Reporting Guidance
<p>15/CMP.1 annex II.E paragraph 32.(c)</p> <p>Change to database or the capacity of national registry</p>	<p>Provide a high level description for each change, reasons for the change and attach in annex 6 test plans and test reports and readiness documentation impacted by the changes.</p> <p>Examples of relevant changes:</p> <ul style="list-style-type: none"> • A major change of the registry operating system platform or the database vendor; • A major change of the registry hardware infrastructure; • A change of the registry software provider. <p>If a change is reported, updated content for the appropriate sections (bolded text in appendix 7) of the following Readiness documents must be provided. If a given document or section is not relevant to the change(s), the Party should provide a statement describing why no modifications were required for that document or section;</p> <ul style="list-style-type: none"> • Database and Application Backup plan – see appendix 7. • Disaster Recovery plan – see appendix 7. • Test Plan – see appendix 7. • Test Report – see appendix 7. <p>Or</p> <p>If no change occurred, indicate no change in this submission. Suggested text for the NIR submission if no change occurred, “No change to the database or to the capacity of the national registry occurred during the reported period”.</p>
<p>15/CMP.1 annex II.E paragraph 32.(d)</p> <p>Change of conformance to technical standards</p>	<p>Provide a high level description for each change, reasons for the change, and attach in annex 6 test plans, test reports and updated registry readiness documentation relevant to the changes.</p> <p>Examples of relevant changes:</p> <ul style="list-style-type: none"> • A major release of the registry software; • A major release under the release management common operational procedure and obtained re-certification from the release manager. <p>If a change is reported, updated content for the appropriate sections (bolded text in appendix 7) of the following Readiness documents must be provided. If a given document or section is not relevant to the change(s), the Party should provide a statement describing why no modifications were required for that document or section;</p> <ul style="list-style-type: none"> • Version Change Management – see appendix 7. • Test Plan – see appendix 7. • Test Report – see appendix 7. <p>Or</p> <p>If no change occurred, indicate no change in this submission. Suggested text for the NIR submission if no change occurred, “No change in the registry’s conformance to technical standards occurred for the reported period”.</p>

Reporting Item	Reporting Guidance
<p>15/CMP.1 annex II.E paragraph 32.(e)</p> <p>Change of discrepancies procedures</p>	<p>Provide a high level description for each change to remove discrepancies and reasons for the change. Party should attach in annex 6 the revised or new procedures relevant to the changes and evidence of successfully applying it. If the change resulted in an update of the registry readiness documentation, then that part of the readiness documentation should be resubmitted.</p> <p>Examples of reported changes:</p> <ul style="list-style-type: none"> • Introduction of additional manual processes to minimise discrepancies or remove problems. Party would need to attach the new or amended procedures and a proof of its successful application; • Change of the software to remove a root cause for discrepancies. Party would need to attach test plans and test reports to show successful implementation of the change. <p>If a change is reported, updated content for the appropriate sections (bolded text in appendix 7) of the following Readiness documents must be provided. If a given document or section is not relevant to the change(s), the Party should provide a statement describing why no modifications were required for that document or section;</p> <ul style="list-style-type: none"> • For procedural changes, Operational Plan – see appendix 7. • For software changes, Test Plan – see appendix 7. • For software changes, Test Report – see appendix 7. <p>Or</p> <p>If no change occurred, indicate no change in this submission. Suggested text for the NIR submission if no change occurred, “No change of discrepancies procedures occurred during the reported period”.</p>

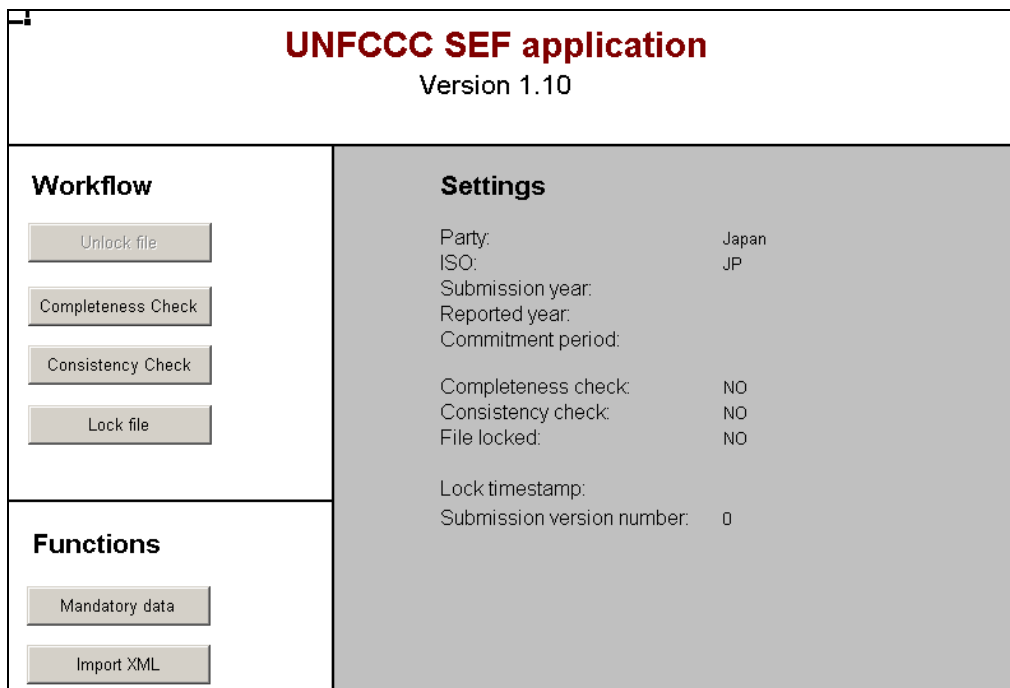
Reporting Item	Reporting Guidance
<p>15/CMP.1 annex II.E paragraph 32.(f)</p> <p>Change of security</p>	<p>Provide a high level description for each change to prevent unauthorized manipulations at the system level and at the user level. Also provide reasons for the change. Attach in annex 6 the new procedures, test plans, and results relevant to the changes and evidence of successfully applying it.</p> <p>Examples of reported changes:</p> <ul style="list-style-type: none"> • Major change to the security of the registry site or the technology underpinning the National Registry; • Changes to the security procedures submitted as part of the readiness documentation. <p>If a change is reported, updated content for the appropriate sections (bolded text in appendix 7) of the following Readiness documents must be provided. If a given document or section is not relevant to the change(s), the Party should provide a statement describing why no modifications were required for that document or section;</p> <ul style="list-style-type: none"> • Security Plan – see appendix 7. • Operational Plan – see appendix 7. <p>Or</p> <p>If no change occurred, indicate no change in this submission. Suggested text for the NIR submission if no change occurred, “No change of security measures occurred during the reporting period”.</p>
<p>15/CMP.1 annex II.E paragraph 32.(g)</p> <p>Change of list of publicly available information</p>	<p>Provide changes as compared to last submission regarding the type of information to be made public pursuant to part E of the annex to 13/CMP.1, paragraphs 44 to 48 inclusive. Changes to the type of information made public may include disclosing information that was previously confidential or not disclosing information anymore because it has become confidential. See the separate guidance document on public information as required under section E of the annex to 13/CMP.1 for more information: "SIAR Publicly Available Information Reporting Guidance for National Registries."</p> <p>Or</p> <p>If no change occurred, indicate no change in this submission. If no change, the Party should clearly state clearly that no change regarding the publicly accessible information pursuant to decision 13/CMP.1, paragraphs 44 to 48 inclusive took place during the reporting period. For all clarity, this covers cases where previously confidential information remained confidential during the reporting period (i.e., no change occurred). Suggested text for the NIR submission if no change occurred, “No change to the list of publicly available information occurred during the reporting period”.</p>
<p>15/CMP.1 annex II.E paragraph 32.(h)</p> <p>Change of Internet address</p>	<p>Provide a description of the change compared to last submission of the National Registry’s Internet address</p> <p>Or</p> <p>If no change occurred, indicate no change in this submission. Suggested text for the NIR submission if no change occurred, “No change of the registry Internet address occurred during the reporting period”.</p>

Reporting Item	Reporting Guidance
<p>15/CMP.1 annex II.E paragraph 32.(i)</p> <p>Change of data integrity measures</p>	<p>Provide a high level description for each change, the reason for the change, and in annex 6, attach the revised procedures and a proof of its successful application.</p> <p>Examples of reported changes:</p> <ul style="list-style-type: none"> • Major revision of Disaster Recovery plans; • A change of Disaster recovery site; • A major change to the database backup tools. <p>If a change is reported, updated content for the appropriate sections (bolded text in appendix 7) of the following Readiness documents must be provided. If a given document or section is not relevant to the change(s), the Party should provide a statement describing why no modifications were required for that document or section;</p> <ul style="list-style-type: none"> • Application Logging documentation – see appendix 7. • Disaster Recovery Plan – see appendix 7. • Test Plan – see appendix 7. • Test Report – see appendix 7. <p>Or</p> <p>If no change occurred, indicate no change in this submission. Suggested text for the NIR submission if no change occurred, “No change of data integrity measures occurred during the reporting period”.</p>
<p>15/CMP.1 annex II.E paragraph 32.(j)</p> <p>Change of test results</p>	<p>The Party does not need to repeat any information that was supplied in the above submission items. If any additional test plans and results are supplied, provide a high level description for each change, reasons for the change and attach in annex test plans and test reports relevant to the changes.</p> <p>If a change is reported, updated content for the appropriate sections (bolded text in appendix 7) of the following Readiness documents must be provided. If a given document or section is not relevant to the change(s), the Party should provide a statement describing why no modifications were required for that document or section;</p> <ul style="list-style-type: none"> • Test Plan – see appendix 7. • Test Report – see appendix 7. <p>Or</p> <p>If no change occurred, indicate no change in this submission. Suggested text for the NIR submission if no change occurred, “No change of test results occurred during the reporting period”.</p>
<p>The previous Annual Review recommendations</p>	<p>Provide each recommendation from the previous annual review recommendation that is relevant to the national registry and provide explanation of how the recommendation was addressed.</p> <p>Previous annual reviews are available on the UNFCCC website: http://unfccc.int/national_reports/annex_i_ghg_inventories/inventory_review_reports/items/4400.php</p>

Appendix 1 – Report R-1: Standard Electronic Format (SEF)

As per decisions 14/CMP.1 and 15/CMP.1, the standard electronic format (SEF) is an essential part of submission under Article 7.1 of the Kyoto Protocol. It is designed to facilitate reporting of Kyoto Protocol units by Parties included in Annex I to the Convention and review of Kyoto Protocol units. These submissions must be made annually. The paragraph 11 of decision 15/CMP.1 outline what Parties are required to submit, and decision 14/CMP.1 details the format of the tables that are to be submitted.

The SEF Application Main Page



UNFCCC SEF application	
Version 1.10	
Workflow	Settings
<input type="button" value="Unlock file"/>	Party: Japan
<input type="button" value="Completeness Check"/>	ISO: JP
<input type="button" value="Consistency Check"/>	Submission year:
<input type="button" value="Lock file"/>	Reported year:
	Commitment period:
	Completeness check: NO
	Consistency check: NO
	File locked: NO
	Lock timestamp:
	Submission version number: 0
Functions	
<input type="button" value="Mandatory data"/>	
<input type="button" value="Import XML"/>	

The SEF reporting format is elaborated under the RSA Forum SEF working group and is not described in this document.

The latest specifications are available at:

https://quickplace.unfccc.int/QuickPlace/itl-rsa/Main.nsf/h_BA5EDCDF5FB9A20AC1257498002A3C21/5388585cc87b433cc1257498002a7358/?OpenDocument

Appendix 2 – Report R-2: List of Discrepant Transactions

The list of discrepant transactions is an essential part of the SIAR submission by a Party, which should be provided in Microsoft Excel format respecting the layout identified in the figure below:

Layout for the List of Discrepant Transactions

DES Response Code	Average number of occurrences 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
<Response Code 1>										
		
			<Serial 1>
								<Serial 2>
								<Serial 3>
		
<Response Code 2>										
		
		

Reporting Requirements

I. Layout and General Requirements

1. The report is structured per DES response code, which should appear in ascending order.
2. Each transaction, which resulted in a response code listed below (see “Applicable DES response code” below), must be listed under the response code, in ascending order.
3. Each transaction finalized during the reporting period should be considered. If a transaction was started but is not yet finalized as of 31 Dec 24:00 of the reported year, it should not be considered for the purpose of this report.
4. If a transaction results in several response codes listed below being returned, the transaction shall appear once under each response code heading.
5. If several unit blocks are affected by the response code, the transaction shall appear once, listing all affected unit blocks in ascending order.

II. Column Requirements

6. DES response codes shall be presented in DES format.
7. Average number of occurrences per transaction for the reported year should be a positive real number, with a precision of 2 digits (ex: 13.07). The average number of occurrences of the response code per transaction for the reported year is equal to the total number of occurrences of the response code for the reported year (in response to transactions proposed by the registry) multiplied by 100.000 divided by the total number of transactions proposed by the registry during the reported year. The result should be rounded up.
8. Average number of occurrences per transaction prior to reported year should be a positive real number, with a precision of 2 digits (ex: 13.07). The average number of occurrences of the response code per transaction prior to the reported year is equal to the total number of occurrences of the response code prior to the reported year (in response to transactions proposed by the registry) multiplied by 100.00 divided by the total number of transactions proposed by the registry prior to the reported year. The result should be rounded up.
9. Transaction Number shall be presented in DES format.
10. Proposal date time shall be presented in the following format: YYYY-MM-DD HH:MM:SS.
11. Date and time shall refer to the date and time of the proposal by the registry and use the UTC reference time.
12. Transaction type shall be one of “Issuance”, “Conversion”, “External Transfer”, “Cancellation”, “Retirement”, “Replacement”, “Carry-over”, “Expiry Date Change”, “Internal transfer”. Quotes shall be omitted.
13. Final state shall be one of “Completed”, “Terminated”, “Cancelled”, “Failure by the initiating registry to terminate the transaction”, or “Other”. Quotes shall be omitted.
14. “Other” shall be used to report internal final states a registry may use when altering transaction status following a manual intervention.
15. Explanation is a free text field a Party may provide explaining why the transaction was not terminated although a response code was returned. It is not expected that a Party provides an explanation if the transaction final state is “Terminated”.
16. Serial numbers shall use the following format: two letters, ISO-3166 code of the country, followed by a dash, followed by the unit block start, followed by a dash, followed by the unit block end; leading zeroes shall be omitted from the block start and end (ex: ZZ-15001-20000).

17. Unit Type shall be one of “AAU”, “ERU (AAU)”, “ERU (RMU)”, “RMU”, “CER”, “ICER”, “tCER”. Quotes shall be omitted.

18. Quantity shall be a positive integer with no leading zeroes.

Applicable DES Response Codes

The following DES response codes are considered to be a discrepancy for the purpose of this report:

Response Code	Check Name	Check Category	Check Description	Transaction Type
4003	Registry Holds Units	General Transaction	Units identified in the transaction must be held by Initiating Registry.	All
4004	Unit Block Attributes	General Transaction	All attributes of all unit blocks must be consistent with ITL unit block attributes except where attributes are changed by the current transaction.	All
4010	Units are Unavailable	General Transaction	Units identified in the transaction must not be involved in another transaction.	All
4011	Units are Cancelled	General Transaction	Cancelled units must not be subject to further transactions.	All
4012	Units are Retired	General Transaction	Retired units must not be subject to further transactions.	All
4014	Units Previously Used in Replacement	General Transaction	Units previously used to replace tCERs or ICERs must not be subject to further transactions.	All
4015	ICER Transaction Ineligibility	General Transaction	ICERs must not be transferred to a holding or retirement account where the CDM Executive Board has notified a replacement requirement for the associated Project.	All
5008	AAU Issuance Quantity	Transaction-specific	The quantity of AAUs issued must not exceed allowed quantity for the Commitment Period.	Issuance
5009	RMU Issuance Quantity	Transaction-specific	The quantity of RMUs issued for each LULUCF Activity Type must not exceed the allowed quantity for that LULUCF Activity Type and Commitment Period.	Issuance
5018	RMU Issuance Limit for Forest Management	Transaction-specific	The quantity of RMUs issued for LULUCF Activity Type 3 (forest management) must not exceed the Party's Forest Management cap, plus net cancellations for activity types 1 and 2 up to a limit of 165,000,000 units.	Issuance
5053	Conversion Eligibility (Track 1)	Transaction-specific	If the unit is a Track 1 ERU, the Party of the Initiating Registry must be determined to meet eligibility criteria 1 through 6.	Conversion
5054	Conversion Eligibility (Track 2)	Transaction-specific	If the unit is a Track 2 ERU, the Party of the Initiating Registry must be determined to meet eligibility criteria 1, 2 and 4.	Conversion
5056	Conversion Unit Type	Transaction-specific	Units for conversion must be AAUs or RMUs.	Conversion

Response Code	Check Name	Check Category	Check Description	Transaction Type
5061	Track 2 ERU Conversion Quantity	Transaction-specific	Track 2 ERU Conversion for each Track 2 JI Project must not exceed the quantity specified by the Joint Implementation Supervisory Committee.	Conversion
5101	General Transferring Registry Eligibility for External Transfers	Transaction-specific	The Party of an initiating national registry must be determined to meet eligibility criteria 1 through 6, except for the first external transfer of a track 2 ERU which the Registry has converted or for transfers to the Excess Issuance Cancellation Account at the CDM Registry.	External
5102	ERU Track 2 Transferring Registry Eligibility for External Transfers	Transaction-specific	If the transaction is the first external transfer of a track 2 ERU which the Registry has converted, the Party of the initiating national registry must be determined to meet eligibility criteria 1, 2 and 4.	External
5103	Acquiring Registry Eligibility for External Transfers	Transaction-specific	The Party of an acquiring national registry must be determined to meet eligibility criteria 1 through 6, except for transfers initiated by the CDM Registry or for transfers to the Excess Issuance Cancellation Account at the CDM Registry.	External
5104	Commitment Period Reserve	Transaction-specific	The total quantity of all units held in a national registry, which may be used for compliance for the applicable Commitment Period of a transaction, must not fall below the CPR level for the Party for that Commitment Period, except where the transaction is a first transfer of Track 2 ERUs converted by the registry or a transfer to the Excess Issuance Account in the CDM Registry.	External
5106	Suspension from making external transfers	Transaction-specific	The Party of an initiating national registry must not have been suspended from making external transfers as a result of not meeting its emission target for the previous Commitment Period.	External
5156	tCER and ICER Cancellation to Net Source and Non-compliance Cancellation Accounts	Transaction-specific	tCERs and ICERs cannot be transferred to Net Source Cancellation Accounts or Non-compliance Cancellation Accounts.	Cancellation
5209	Quantity of Replacement Units	Transaction-specific	The quantity of units replaced must equal the quantity of replacing units.	Replacement
5211	Location of Replaced tCERs	Transaction-specific	tCERs to be replaced must be held in a Retirement account or a tCER Replacement account.	Replacement
5212	Location of Replaced ICERs	Transaction-specific	ICERs to be replaced must not be held in Cancellation accounts.	Replacement
5213	ICER Replacement Units (upon Expiry)	Transaction-specific	ICER Replacement accounts (upon expiry) cannot acquire tCERs or ICERs.	Replacement
5214	tCER Replacement Units	Transaction-specific	tCER replacement accounts (for unit	Replacement

Response Code	Check Name	Check Category	Check Description	Transaction Type
	(upon Expiry)	specific	expiry) cannot acquire ICERs.	
5215	ICER Replacement Units (upon Reversal of Storage or Lack of Certification Report)	Transaction-specific	ICER Replacement accounts (for Reversal in Storage) may not acquire tCERs and may not acquire ICERs with a Project Number other than that specified in the replacement notification.	Replacement
5220	Project ID for ICERs Replacement (upon Reversal of Storage or lack of Certification Report)	Transaction-specific	For ICER replacement transactions upon Reversal of Storage or lack of a Certification Report, the Project ID for the ICERs to be replaced must be consistent with the Project ID contained in the replacement notification.	Replacement
5255	CER, tCER and ICER Retirement Eligibility	Transaction-specific	The Party of the Initiating Registry must be determined to meet eligibility criteria 1 through 6.	Retirement
5256	tCER and ICER Retirement Limit	Transaction-specific	tCER and ICER retirement must not exceed allowed quantity.	Retirement
5301	National Registry Carry-over	Transaction-specific	The Initiating Registry carrying over units must be a national registry.	Carry-over
5304	Units Available for Carry-over	Transaction-specific	The quantity of units carried-over must not exceed the limit for carry-over established by the Compliance Committee for the Party and reported to the registry in the Unit Carry-over notification.	Carry-over
5305	RMU Carry-over	Transaction-specific	RMUs may not be carried over.	Carry-over
5306	ERU (from RMUs) Carry-over	Transaction-specific	ERUs converted from RMUs may not be carried over.	Carry-over
5307	ICER or tCER Carry-over	Transaction-specific	tCERs or ICERs may not be carried over.	Carry-over
5312	ERU Carry-over Quantity	Transaction-specific	The quantity of ERUs (which have not been converted from RMUs) carried-over by the Party must not exceed 2.5% of that Party's allowed quantity of AAU issuance for the Commitment Period.	Carry-over
5313	CER Carry-over Quantity	Transaction-specific	The quantity of CERs carried-over by the Party must not exceed 2.5% of that Party's allowed quantity of AAU issuance for the Commitment Period.	Carry-over

Example Report

The figure below contains an example report for the list of discrepant transactions.

Example Report for the List of Discrepant Transactions

DES Response Code	Average number of occurrences 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
4003	2.53	2.34								
			ZZ1	12/10/2008 22:00:04	Conversion	Terminated		ZZ-1001-2000	RMU	1000
			ZZ2	13/10/2008 13:13:45	External Transfer	Terminated		ZZ-2001-3000	AAU	1000
								ZZ-3001-5000	AAU	2000
4004	3.12	2.71								
			ZZ3	08/08/2008 11:11:22	Retirement	Cancelled	Registry was offline for 22 hours	ZZ-10001-20000	CER	10000
			ZZ4	08/08/2008 11:11:24	Retirement	Cancelled	Registry was offline for 22 hours	ZZ-20001-30000	CER	10000

Appendix 3 – Report R-3: List of CDM Notifications

The list of CDM notifications received by a registry during the reported year is an essential part of the SIAR submission by a Party, which should be provided in Microsoft Excel format respecting the layout identified in the figure below:

List of CDM Notifications

Notification Type	Notification Number	Notification Date Time	Target Number of Units	Number of Units Canceled	Number of Units Replace	Difference		Explanation
						At target date	Post target date	
<Notification Type>								

<Notification Type>								

This report lists the notifications received by a registry during the reported year and should only consider CDM related notifications.

The corresponding DES notification types are as follows:

Notification Type Code	Description
3	Impending Expiry of tCER or ICER
4	Reversal of Storage for CDM Project
5	Non-submission of Certification Report for CDM Project

Reporting Requirements

I. Layout and General Requirements

1. The report is structured per notification type, which should appear in ascending order and must not be repeated for the same ITL notice type.
2. Each notification number must be reported under its notification type, order by ascending notification date time.
3. Only notification where the message date of the initial notification (field “messageDate” of the ITLNotice message) is within the reported year should be reported.
4. This report should not be produced before the first of February and should contain all cancellations and replacements made during January for notification received during the previous year.

II. Column Requirements

5. Notification type must be one of “Impending Expiry”, “Reversal of Storage” or “Non-Submission of Certification Report”.
6. Notification Number must be in DES format.

7. Notification date time must match the “messageDate” field of the initial notification and must respect the following format: YYYY-MM-DD HH:MM:SS.
8. Target number of units must be a positive integer corresponding to the initial target set by the notification.
9. Number of units cancelled must be a positive integer corresponding to the number of units cancelled in fulfilment of the notification prior to or after the target date set by the notification.
10. Number of units replaced must be strictly positive integer corresponding to the number of units replaced prior or after the target date set by the notification.
11. Difference between target and cancellations or replacements at target date must be equal to the initial target of the notification less cancellations and replacements made to fulfil the notification requirements at the target date.
12. Difference between target and cancellations or replacements post target date must be equal to the initial target of the notification less cancellations and replacements made to fulfil the notification requirements at the report date.
13. Explanation is a free text Parties should provide when not undertaking a replacement at the time of the report.

Example Report

The figure below contains an example report for the list of CDM notifications. Additional notes are provided illustrating the most frequent cases.

Example of List of CDM Notifications Report

Notification Type	Notification Number	Notification Date Time	Target Number of Units	Number of Units Cancelled	Number of Units Replaced	Difference between target and cancellations or replacements		Explanation
						At target date	Post target date	
Impending Expiry for tCER or ICER								
	331	23/10/2008 15:56:17	1000	0	1000	0 (1)	0	
	332	24/10/2008 22:56:17	2000	0	2000	500 (2)	0	
	333	25/10/2008 15:36:17	3000	0	500	2500 (3)	2500	Registry down post target date
Reversal of Storage for CDM Project								
	334	23/10/2008 08:56:17	1000	300	700	0	0	
	335	21/11/2008 15:56:17	2000	1500	1500	-1000 (4)	-1000	
Non-submission of certification report								
	336	19/12/2008 15:56:17	3000	0	0	3000 (5)	3000	Registry down
(1) The notification was fulfilled in time (before or at the target date) (2) Only 1500 units were replaced on time; at the time of the report the 2000 units were replaced (3) Only 500 units were replaced on time and at the time of the report - the notification is unfulfilled (4) Too many units were cancelled or replaced before or at the target date (5) No cancellations or replacement were performed to fulfill the notification, either at or post the target date								

Reporting Requirements

I. Layout and General Requirements

1. The report is structured in two parts: the first part contains the list of non-replacements following a reversal of storage, impending expiry of ICER or tCER or non-submission of certification report; the second part contains the details for each notification listed.
2. The notifications to report are those in report R-3 above that were not fulfilled at the report date.
3. The relevant information from report R-3 shall be replicated in this report for each notification.
4. Units concerned shall be reported for each notification; units concerned are:
 - For impending expiry notification, the units provided by the ITL in its initial notification.
 - For reversal of storage and lack of certification notifications, the units issued for the project notified by the ITL in the initial notification.
5. Units concerned shall be reported in the same manner as report R-3 (“abbreviated format”).
6. Non-replacement records shall be sorted in ascending order of notification number.
7. Units concerned shall be sorted in ascending order or the serial number of the units.

II. Column Requirements

8. See reports R-3 (and R-2 for the units concerned).

Example Report

The figure below contains an example report for the list of non-replacements report.

Example Report for Non-replacements

<i>List of non replacements for reversal of storage, non-submission of certification report and impending expiry of ICER or tICER</i>								
Notification Type	Notification Number	Notification Date Time	Target Number of Units	Number of Units Cancelled	Number of Units Replaced	Difference between target and cancellations or replacements		Explanation
						At target date	Post target date	
Reversal of Storage for CDM Project								
	333	25/10/2008 15:36:17	3000	0	500	2800	2500	Registry down post target date
	444	26/10/2008 15:36:17	2000	0	300	1900	1700	Registry down post target date
Non-submission of certification report								
	336	19/12/2008 15:56:17	3000	0	0	3000	3000	Registry down
<i>Non-replacement record for reversal of storage</i>								
Notification Number	Notification Type	Notification Date Time	Target Number Of Units	Number of Units Cancelled	Number Of Units Replaced	Difference between target and		Explanation
						At target date	Post target date	
333	Reversal of Storage for CDM Project	25/10/2008 15:36:17	3000	0	500	2800	2500	Registry down post target date
						Units concerned		
						Serial Number	Unit Type	Quantity
						ZZ-1-2000	ICER	2000
						ZZ-5001-5600	ICER	600
						ZZ-20001-20400	ICER	400
<i>Non-submission of certification report</i>								
Notification Number	Notification Type	Notification Date Time	Target Number Of Units	Number of Units Cancelled	Number Of Units Replaced	Difference between target and		Explanation
						At target date	Post target date	
336	Non-submission of certification report	19/12/2008 15:56:17	3000	0	0	3000	0	Registry down
						Units concerned		
						Serial Number	Unit Type	Quantity
						ZZ-10001-11000	ICER	1000
						ZZ-12001-14000	ICER	2000
<i>Non-replacement record for reversal of storage</i>								
Notification Number	Notification Type	Notification Date Time	Target Number Of Units	Number of Units Cancelled	Number Of Units Replaced	Difference between target and		Explanation
						At target date	Post target date	
444	Reversal of Storage for CDM Project	26/10/2008 15:36:17	2000	0	300	1900	1700	Registry down post target date
						Units concerned		
						Serial Number	Unit Type	Quantity
						ZZ-7001-9000	ICER	2000

Appendix 5 – Report R-5: List of Invalid Units

The list of invalid units is an essential report under the SIAR that should be provided by Parties in Microsoft Excel format. The report structure is depicted in the figure below:

List of Invalid Units Report Layout

Serial Number	Unit Type	Quantity	Transaction Number

Parties should report any units subject to a transaction receiving a notification for discrepancy from the ITL that the registry has failed to terminate at 31 December 24:00. If a registry did not receive such a notification by 31 December 24:00, or it has terminated or cancelled all such transactions, it should not report the units involved in the transaction.

Reporting Requirements

I. Layout and General Requirements

1. The report is a list of serial numbers, unit type, quantity, and transaction number.
2. The serial numbers shall be ordered ascending.
3. The format of serial number, unit type, quantity and transaction number are those of report R-2.
4. The transaction number is the first transaction that failed to terminate involving the units listed on that row.

Appendix 6 – Further Detailed Information about Reporting Changes to National Registry

What should be reported as a change?

This section provides guidance on what should be reported as a change to a national registry. This strikes a balance between the requirement to report any change and the assessment by the expert review team of significant changes. This is described in the decisions as follows:

- Paragraph 22 of the annex to decision 15/CMP.1 “Each Party included in Annex I with a commitment inscribed in Annex B shall include in its national inventory report information on **any changes** that have occurred in its national registry, compared with information reported in its last submission, including information submitted in accordance with paragraph 32 of these guidelines;
- Paragraph 114 of the annex to decision 22/CMP.1 “The expert review team shall review the information submitted as supplementary information under Article 7, paragraph 1, and shall identify any **significant changes** in the national registry reported by the Party or any problems identified by the expert review team in the course of the review of ERUs, CERs, tCERs, ICERs, AAUs and RMUs and transaction log records that may affect the performance of the functions contained in the annex to decision 13/CMP.1, the annex to decision 5/CMP.1 and the adherence to the technical standards for data exchange between registry systems in accordance with relevant COP/MOP decisions. This review should take place in conjunction with the annual review in accordance with the relevant procedures in paragraphs 115 to 117 below.”

Parties must report at least the significant changes, however reporting every change would lead to excess amounts of information to be assessed. Release management practices suggest a means of managing the volume of information.

Changes to national registries are managed and tested in accordance with the plans developed by the registry as required by section 9.2 of the data exchange standards. Changes typically not made individually, but as collection of changes are known as a release. A release is normally tested and promoted to a live environment as a whole, and the test plans and reports for a release will form part of the registry readiness documentation described in appendix 7 below. So registries should not report each individual change within a release, but they should report releases as a whole, using the following definition to help determine what changes within the release might be deemed significant.

Definition: A Significant Change is a change requiring a large implementation effort by the registry software developer or involving large risks or impact to the registry development and/or operation.

In terms of a release the changes that might be deemed significant are likely to account for the majority of the effort of the release. The changes might not necessarily involve change to the registry software, but significant change to the environment in which the registry operates. Some examples are:

- Change of the registry software to adapt to a major new version of the data exchange standards;
- Change of the data centre used to host the registry, which might involve no change to the registry software but considerable effort in testing that it functions as expected in the new environment;
- Upgrade of the components that support communication with the ITL.

Baseline for Reporting Changes

The baseline for reporting changes of the national registry is the information provided by the Party in its last NIR submission. For the first annual submission, the last submission will be the Initial Report and the readiness documentation submitted under the Initial Independent Assessment common operational procedure. Annual submissions are posted on the UNFCCC website:
http://unfccc.int/national_reports/annex_i_ghg_inventories/inventory_review_reports/items/4400.php

Most of the relevant information regarding the non-functional requirements for registry software, infrastructure and procedures has been initially submitted by Parties in the registry readiness documentation set, which was one of the three key items, along with connectivity testing and interoperability testing, on

which the Initial IAR assessment was based. The purpose of the registry readiness documentation is to show that non-functional requirements of the DES are met. In addition, these requirements ensure the Party has an adequate plan for addressing operational and security requirements of its national registry.

The Party's annual submission shall therefore include a description of any significant changes made to its national registry as compared to its previously submitted readiness documentation and its initial report. The initial readiness documentation did not include information on changes made to minimize or remove discrepancies (decision "15/CMP.1 annex I.E paragraph 17"), as at that time no discrepancies existed. Information on those change categories - if applicable - must be part of the annual submission.

General Guidance on Reporting Changes

Changes affecting the registry readiness documentation should result in the resubmission of the documentation that has changed as part of the Party's annual submission. If updated readiness documentation has been previously submitted to the ITL Service Desk or ITL Administrator, it should still be included as part of the Party's annual submission.

The re-submission of this readiness documentation serves two purposes:

- a) To ensure coherent review of change in all impacted areas;
- b) To provide a consistent baseline for evaluation and review for next annual submission.

Party must submit their amended readiness documentation to demonstrate their successful implementation of the change. The readiness documentation should include the elements described in appendix 7 of this document.

Parties should also report all the changes that can be considered significant changes in their annual submission, consistent with the above definition of "Significant Changes," as well as the examples given in the following section should assist Parties in reporting the changes to their national registry.

Appendix 7 – Readiness Documentation Reporting Guidelines

Section 3 contains guidance on content to include in the NIR submission for changes to the Party's national registry during the reporting period. This should be used as the basis of the Party's submission for the national registry specific content of its annex 6 to the NIR.

When to Report Changes to the Registry Readiness Documentation

Changes to the registry readiness documentation should be resubmitted if:

1. The national registry underwent significant change(s) as discussed on section 3.2 and appendix 6 of this document.
2. The national registry experienced corrective actions following problems or discrepancies discussed in section 3.1.

How to Report Changes to the Readiness Documentation

If Party reported corrective actions to resolve discrepancies as described in section 3.1 or if the readiness documents changed due to significant changes or actions as described in section 3.2, revised readiness documentation will need to be submitted. Those documents should be submitted once as part the annual submission. For example, if several changes or corrective actions resulted in updates of the security plan, the security plan should only be submitted once as part of the next NIR submission.

The amended readiness documents can be attached to the submission as annex 6 to the Party's NIR.

Language to Use When Reporting Updated Readiness Documentation

Updated registry readiness documentation must be submitted in English, with the following exception.

For test results and test cases:

A summary of the test results and test cases must be provided in English and the detailed test results should be made available in native language.

Or

The detailed test results and test cases must be provided in English.

Specific guidance for reporting on user-authentication mechanism

As part of the security plan of its national registry, RSAs should report on user-authentication mechanism. In order to facilitate the assessment, it is strongly recommended that RSAs refer, in their submission, to one of the authentication method and on additional improvements to user-authentication, as described below. Note that if a registry uses one of the method outlined below for the authentication of its end users, it is sufficient for the relevant RSAs to refer to that method (i.e. no further description is needed) :

Method 1: two-factor authentication

Two-factor authentication designates an authentication scheme involving at least two factors of identity to be verified. The factors being something the user:

- knows (knowledge factor) e.g. userid/password, PIN.
- has (ownership factor) e.g. individual digital certificate, security token, cell phone number.
- is (inherence factor) e.g. fingerprint, retinal pattern, voice, other biometric identifier.

Currently all registries implement at least userid/password, therefore have the first factor of authentication.

Some registries already implement a second factor of authentication from the prescribed list, for all users, other implement a second factor of authentication only for a subset of their users.

In practical terms, using the inherence factor is very costly and difficult to implement as it involves biometric security mechanisms. Therefore it is recommended to focus on the ownership and knowledge factors. Two-factor authentication methods include, for example:

- Login/password + token: the user knows a login and password, and is equipped with a synchronous security token device.
- Login/password + SMS: the user knows a login and password, and receive a SMS containing a one time password which is required in order to propose a transaction.
- Login/password + certificate: the user knows a login and password, and needs a digital certificate to access the registry application or to propose a transaction.
- Certificate + password: the users has a digital certificate, and must enter the matching password on each connection to the registry application or on each transaction proposal.

It is highly recommended for systems submitting transactions to a registry application to implement two-factor authentication for the connection of their users.

Method 2: two-man rule / additional authorised representative

Enforcing the two-man rule would mean that a transaction, to be actually proposed to the ITL by the national registry, needs approval from two authorized users.

This mechanism does not involve changing the current authentication mechanisms, but aims at mitigating the risk of unauthorized transactions by enforcing the need for two account representatives to authorize a transaction. Therefore, should one user's log-on credential be compromised, this would not be sufficient to propose a fraudulent transaction.

The two-man rule/additional authorised representative is currently available as an optional requirement within EU-ETS Registries. Technically, this is not an overly complex mechanism to implement, although it does have an administrative impact. This mechanism would however represent a satisfactory authentication improvement for Registries with comparably low user numbers and transactional activity.

Method 3: paperwork / stringent processing of transaction proposal by RSA

This option involves supporting each transaction proposed to the registry application, either electronically or on paper, by a duly completed form physically submitted to the RSA.

When being proposed within the registry system, the transaction is considered on hold, and therefore not sent to the ITL, until the form is received.

Upon receipt and validation of the form, the transaction is formally approved. The Registry Administrator can therefore "unpause" the transaction, which is then actually sent to the ITL by the registry application. The validation of the form needs to be carried out by the RSA in a stringent manner. In particular, it is crucial to ensure authenticity of the entity proposing the transaction on the basis of, inter alia, legal proof of the entity's existence or digital certificate unique to it. This mechanism will be more effective when implemented with the complementary measure for customer control, as described below.

This method involves a delay in the transaction processing and an increase of administrative overhead necessary to manage the forms. It is however not complex from a technical implementation perspective, and would represent a satisfactory authentication improvement for Registries having a low transaction volume.

Additional improvements to use authentication

RSAs are also strongly encouraged to put in place and report on additional improvements. These improvements cannot replace one of the 3 methods proposed above, but should be seen as complementary measures by registries willing to achieve an higher level of security.

Complex passwords

Implementing complex password rules involving mechanisms such as special characters, or entry of random characters of the password, is possible in order to reduce the ability of the attacker to guess a password, to make the password more resilient to keylogging and to make the passwords less vulnerable to a brute force attack.

The complexity must be balanced with the ease of use and the ability of a human being to remember a complex password. Overcomplex password will end up written on post-its below the users keyboard, which is eventually going against the intended goal.

A good password policy can also help in achieving a better security level by, for example, renewing the passwords on a regular basis while preventing the use of already used passwords.

Customer control

Ensuring the accounts are held by real natural or legal persons helps by reducing the ability to create a “fake” account used solely for fraudulent purposes.

Checking the existence of the entities and enforcing a more stringent control during the process managing the opening of a person holding account helps in achieving a better security. It can however be quite complex to achieve a better customer control with foreign entities.

As an example, a national registry currently has implemented restrictions in order to allow a person holding account opening only to its nationals.

Other more robust controls could include the requirement to provide proof of permanent residence in the country of account opening, proof of an open bank account in the country of account opening, proof of legal status of a company, translation of documents into the specified language of the country where the account is to be opened or requirement that all such evidentiary documentation is certified as ‘true’ by a lawyer.

Awareness raising

Providing the registry application users with more information and training regarding the security attacks is one of the most efficient ways to proactively mitigate the risks. In addition to clear and robust account management procedures, users can be educated by highlighting the most common attacks and the ways to prevent them.

Note that test plans and test reports pertaining to changes to user-authentication mechanism have to be provided in the annual submission.

Amended Readiness Documentation

This section contains an amended version of the registry readiness documentation questionnaire, to be used by Parties to submit the update of their national registry procedures as part of their annual submission.

The description for the contents of the readiness documentation has been amended based on the experience gained during the initial registry readiness documentation review.

The bolded points within each section represent the mandatory points that must be reported as a minimum when any change is made and the documentation resubmitted.

Database and Application Backup

Detailed backup plan for the production database and software.

The plan should include:

- a. Scope or content of backup procedures (i.e., database, application software, server logs, and application logs referred to in the section “Application Logging Documentation”).**
- b. Identification of backup hardware and software.
- c. Backup retention periods (note that some application logs should be kept for a period of 15 years – see section 7 of the data exchange standards).**
- d. Frequency of database backups (recommendation: minimum daily) and any method of rolling forward from the point of backup, for example using database log files.**
- e. Personnel responsible for backup (including a primary individual and an alternate, or a staffing plan).
- f. Specific back up schedule and procedures e.g., backup is schedule at 23:00 each day and tapes removed and sent off site by 10:00 the following day.
- g. Identification of backup media and its location.
- h. Strategy to monitor performance of backup tasks, including notification of backup failures, backup log review, spot checks, audit, management reporting.

Disaster Recovery Plan

Designed to enable Registry to survive in the event of catastrophic failure or disruption of the host environment and to re-establish normal business operations as quickly as possible.

The disaster recovery plan should include:

- a. Appropriate strategies to ensure that critical operations can resume normal processing within a reasonable time frame.**
- b. Specific minimum hardware and software requirements to host the registry on a temporary basis. Data recovery procedures allowing backed up data to be recovered. The disaster recovery plan should be explicit regarding:
- c. Which registry data can be recovered and to which point in time it can be recovered.**
- d. Methods used for ensuring data backups and database logs used for recovery are available on the recovery site. Should clearly state if automated tools, such as data replication tools, are used to support this.
- e. Which registry data may be lost during when a disaster occurs.
- f. Periodic testing strategy to demonstrate the effectiveness of the disaster recovery plan.**
- g. Expectation for time frame in which registry could begin operation following a disaster – dependent on the volume of transactions, cost and other factors and is not expected to be the same for each registry.**
- h. Contingency planning, for the eventuality that the primary facility cannot perform required daily operations, should address.
- i. Identification of off-site facility with adequate disk space/storage and availability to serve as an emergency hosting environment.
- j. Off-site location of documentation and procedure manuals, as well as any paper-based forms, necessary to deploy under a Disaster Recovery scenario.
- k. Roles and responsibilities for primary and alternate personnel at the offsite location.
- l. Communication mechanisms to notify all appropriate parties that a contingency plan is in effect (i.e., ITR, other registries or users).

Security Plan

Defined in order to protect the application and data from unrestricted and unsolicited use.

Access to Registry data should be secured at multiple levels to ensure redundancy of protection:

- a. Server security: Web and/or database server should be secured use authenticated access, appropriate assignment of roles and associated rights and also physically secured to prevent unauthorized access to the data and application.
- b. User-authentication security: ensures no unauthenticated access to information in the registry.. See the section “Specific guidance for reporting on user-authentication mechanism” above for details on reporting of this item.
- c. Session security: ensures that data is not intercepted as it is broadcast over the Internet. This is accomplished by encrypting data passed to and from the registry.

The security plan should:

- d. Define rules & responsibilities for security, recognizing that actions by persons are the most significant contributing factor to the success or failure of security planning.
- e. Assign a network and database administrator.
- f. Describe arrangements for personnel screening.
- g. Determine who has physical access to the registry Web, Back End and/or Database servers.**
- h. Determine which audit trails records activities at the Web, Back End and/or Database levels.**
- i. Describe how communications are encrypted: from the registry users to the registry, from the ITL to the registry and between the registry nodes if applicable.
- j. Describe how communications are encrypted: from the registry users to the registry, from the ITL to the registry and between the registry nodes if applicable.**
- k. Describe firewalls and anti-virus measures.**
- l. Describe the password policy (length, formation, duration).**
- m. Describe private keys protection policies.**
- n. Describe how user IDs and passwords are removed or invalidated after users have become inactive.**
- o. Describe which method is used for user-authentication security (see section “Specific guidance for reporting on user-authentication mechanism” above for details)**

Application Logging Documentation

The data exchange standards define information that a registry must log and keep for extended periods of time.

The documentation should include:

- a. A description of the registry data model or file structures used to maintain a transaction log, as defined in section 7.1 of the data exchange standard.**
- b. A description of the registry data model or file structures used to maintain a reconciliation history log, as defined in section 7.2 of the data exchange standard.
- c. A description of the registry data model or file structures used to maintain a notification log, as defined in section 7.3 of the data exchange standard.**
- d. A description of the registry data model or file structures used to maintain an internal audit log, as defined in section 7.4 of the data exchange standard.**
- e. A description of naming convention, medium of storage used to store messages sent and received by the registry, in accordance with section 7.5 of the data exchange standard.
- f. Activity logging that is utilized to track unauthorized attempts to log on to the server as well as general usage.
- g. Assignment of personnel to review activity logs on a regular basis.
- h. A description of the personnel and procedures used to review application logs.

Time Validation Plan

A registry must define and follow specific procedures to validate server time on a periodic basis, for successful data exchange

The plan should include:

- a. Identification of the client software or hardware used as NTP client.**
- b. Version of NTP used.**
- c. Process and frequency of clock correction used and tolerance for discrepancies.
- d. Identification of NTP time server(s).
- e. Assignment of personnel to perform or monitor time validation.
- f. Process used to detect and escalate failures in the NTP process, for example, to correct clocks, identify excess time drift, and identify disagreement between servers and communications failures.
- g. Process for adjusting time in case the time validation process is out of control.

Version Change Management

A clear migration path should exist to upgrade from version to version of registry software and database schemas.

The Version Change Management Plan should include:

- a. A description of how the registry software (binaries and source code if applicable) is versioned and kept track of (naming conventions, directory structures, use of version control system).
- b. A description of how all documentation pertaining to the registry software is versioned and kept track of.
- c. A description of how changes to the registry software are tracked from their inception to their closure.
- d. A description of how changes to the registry software are notified to the registry users, the ITL and relevant STL(s) once they are deployed in production.**
- e. A description of how new versions of registry software are tested prior to their deployment in production. This should include a description of pre-production environments, whether and how test plans are established for the change and whether and how test reports are produced.

Test Plan

Ensures that a registry has performed testing prior to implementing changes to the live registry.

The test plan describes the various levels and types of testing that will be done throughout development. It should include:

- a. Description of overall test strategy, testing procedures and available or foreseen test documentation.**
- b. Identification of Testing tools.
- c. Assignment of personnel to perform testing of the software, both on the initial release and for an upgrade in hardware or software.
- d. Description of test environment(s) and how these environment(s) are managed to ensure that results of testing in test environment(s) replicate the results expected in the production environment.
- e. Evidence that the plan provides for systematic testing in logical order of all module subsystem, and system requirements against a well-defined set of test cases.
- f. Evidence of testing of all user roles supported by the registry (administrator, public user...).
- g. Identification of the test cases that form part of regression tests which are performed on each release.
- h. Description of how test logs are produced and kept. Test logs should contain information on which test cases were run, who run them, at which time, and whether the test case passed or failed; if a test case fails, a reference or description of the incident should be provided.
- i. A description of how incidents following testing are reported and kept track of. Incidents occur when the expected outcome of a test case do not match the actual outcome.

Test Report

Provides evidence that a registry has performed testing

The test report details the various levels and types of testing that have been completed throughout development. It should include:

- a. A summary of all tests that were executed as part of the test plan. The summary should include the number of test cases executed and the number of test cases where an incident was detected.**
- b. For each test case: who ran the test, when and whether it passed or failed.
- c. For each test case where an incident was reported: the description or reference to the incident.

Operational Plan

Ensures that the Registry has appropriately planned and staffed its operational requirements, so that the initial standards and requirements will be addressed on an ongoing basis.

The operational plan should include a description of:

- a. A staffing and management plan including foreseen training, if any.
- b. The ongoing performance evaluations and assessments applicable to the registry system.
- c. The strategy used to modernize the technologies used by the national registry.
- d. The support arrangements: dependencies on 3rd party support providers and service level; agreements.
- e. How licenses are managed.
- f. How patches are applied.
- g. How the registry administrator deal with reconciliation inconsistencies.
- h. How the registry administrator manages incidents, including the tools used.
- i. How the registry administrator deals with changes to the national registry.
- j. How new or updated processes are incorporated into the working operation of the registry.**