WORKSHOP BACKGROUND PAPER No.3

SETTING THE TECHNICAL INFRASTRUCTURE FOR TRANSACTION REGISTRIES

By Frederic Dinguirard

September 2015

NOTE: This Background Paper is a preliminary document with a limited number of copies circulated to stimulate discussion and critical comment at the PMR Technical Workshop *"Building Registries to Support the Next Generation of Carbon Markets"*, September 23-25, 2015 – Sacramento, CA. Written comments and suggestions are welcome and should be sent to the PMR Secretariat (pmrsecretariat@worldbank.org) no later than October 15, 2015.

CONTENT

List of Annexes

List of Tables

List of Figures

INTRODUCTION

This note aims to guide readers through the different steps involved in the development and implementation of the registry technical infrastructure – including the preparation of "tailor-made" registry specifications:

A. Overview of registry procurement steps;
B. Preliminary considerations (i.e. prior to drafting specifications);
C. Functional specifications; and
D. Technical specifications.

This process, and certain steps in particular, may require specific IT project management skills.

A- OVERVIEW OF REGISTRY PROCUREMENT STEPS

1. Request For Interest: Identifying potential registry vendors and their offer

As a first step in registry procurement, a Request For Interest (RFI) – based on clear functional specifications – can be issued and shared with several pre-selected IT/registry providers. Section "C - Functional Specifications" provides practical guidance on the preparation of such functional specifications. The feedback received from interested providers may bring valuable first-hand information and insight – in particular related to:

- Offering and prices;
- Experience and level of expertise;
- Quality of their project management; and
- Capacity to cooperate and deliver expected results in a common working language.

This process also allows making a first assessment of the suitability of different type of delivery models for registry product and services – including "Software as a Service" (SaaS)[1], application/adaptation of an existing software, or development from scratch.

2. Request for Proposal: Specifying registry needs

Following the completion of the RFI process, several registry vendors may have been identified, and the procurement process can move to its next phase, i.e. the Request For Proposal (RFP). A number of stages are involved in the preparation of the RFP:

- Delineating the nature of expected services from vendors based on basic registry needs (see STAGE 1 below);
- Specifying registry business requirements (STAGE 2);
- Specifying registry technical requirements – including the scale and environment of the registry (STAGES 3 and 4).

[1] "Software as a Service" (SaaS) is a software licensing and delivery model in which the software vendor – based on a subscription/fee – hosts and maintains the servers, databases and code that constitutes the registry application. Registry management services may also be offered.

STAGE 1	Delineating the nature of expected services

This first stage is intended to comprehensively specify the services sought from the supplier. A wide range of services and delegation of responsibilities can be envisaged over and above the provision of the registry system (see “mapping registry processes” in Section 2). The list of services expected could be detailed from the indicative elements suggested below.

Regarding the IT system (i.e. the registry):

a. The procurement of a registry in accordance with the functional and technical specifications, and available online;
b. The reversible hosting of data and processing services and the registry site;
c. A secure and confidential infrastructure;
d. Maintenance in operational condition of the IT system: concerns corrective and upgrade maintenance for both the registry and underlying software component versions;
e. A service level agreement, which details the level of commitment to quality and security management including reactivity to change.

Regarding auxiliary services:

f. First level hotline and support to users;
g. Training material, user guides, operating manuals, training courses;
h. The drawing up of "Terms of Use" of the registry including security measures and any limitations (web browsers ...);
i. Management of requests for opening accounts: formal checks, due diligence, opening accounts upon confirmation by the registry administrator, and assigning user authorization;
j. Regular update and review of users related documentation;
k. Invoicing users.

OUTCOME	The scope and objectives of the sought services are defined.

STAGE 2	Specify registry functional/business requirements

This stage is intended to define the business requirements to be included in the registry function (see Section "C-Functional specifications" for more guidance):

a. List the business rules which must be respected (e.g. irreversible nature of a withdrawal);
b. Chart of accounts and accounting models:
    i. Identify the (types of) accounts which are needed for the Market Mechanism to function;
    ii. Imported units (see paragraph "connecting registries"): determine for each type of unit whether to use exclusively a third-party registry, definitive import or mirror accounting. Determine the accounts to include in the chart of accounts;
    c. List the types of operation, and for each type of operation: detail the accounting model (see table "Accounting models: type of accounts debited or credited by type of transaction");
d. List the type of units required:
    i. Detail the format of serial numbers;
    ii. Determine if labels can be associated with units and if so which ones;
    iii. Determine if the serial numbers and / or units are associated with an "issuance year" (vintage) or any other timestamp;
e. Determine the serial number selection rules (LIFO, FIFO ...)
f. Establish a list of user authorization profiles;
g. Establish a list of the functions that the registry must offer
    i. Formalize the workflow for each function;
    ii. Determine the events that initiate each transaction, especially issuance, allocation, and all types of cancellations;
h. Establish a correlation table between functions and user authorization profiles (see Annex of this document);
i. Describe as necessary, any automatic events and detail them:
    i. Certain units may have an expiry date;
    ii. Planned notification of regulatory milestones etc.
j. Draw up templates for all reports to be produced;
k. Detail the registry website structure, requirements for animation and design.

OUTCOME	The "basic" business requirements are specified and reflect functional needs. The Functional/Business Specifications are completed: any registry/IT provider must be able to assess if needs can be addressed with their product and service solutions.

STAGE 3	Specify registry technical requirements (1/2): “scale” of the registry
This stage is intended to size the processing capacity required for the registry. This stage also provides estimates of the staffing requirements to administer the registry (see Section “D-Technical Specifications”): Detailed estimates of the following elements: a. Number of users expected; b. The number of users to train as necessary; c. Number of simultaneous connections to the registry; d. Target number of accounts and number of accounts to open per year; e. Number of accounts expected per year and expected peaks of activity during the year; f. Number of potentially interconnected registries; g. Number of units accounted for and their estimated monetary equivalent; h. Minimum number of technical environments required (production, preproduction, testing ...); i. List of data to archive (logging, audit trail, history available on-line) and the duration for which the archive must be kept (taking into consideration regulatory constraints); Concerning the organization and administration of the registry and data processing services: j. Determine working hours and holidays, hotline opening hours, the times the registry is available on-line (distinguishing as necessary, the hours available for users and those available for administration) determine the number of staff required for the hotline and for registry administration.	
OUTCOME	The “scale” of registry operational requirements are specified: any registry/IT provider selected after the RFI step (i.e. based on the Functional Specifications) must be able to “size” their product and service solutions.

STAGE 4	Specify registry technical requirements (2/2): “environment” of the registry
This stage is intended to detail the technical requirements for systems architecture, security and confidentiality. Putting the registry information system in context (see paragraph “connectivity options”): a. Map out the information systems to connect to the registry (central hub, MRV ...) and draw up an inventory of interfaces between the registry and other systems; b. Exchanges between registries: detail the technical architecture to implement for the transfer of units between registries (via a central hub, peer-to-peer, or both); c. Stipulate whether the registry needs to use a particular communications protocol for certain interfaces notably if the registry must conform to the Data Exchange Standard in order to handle exchanges between registries. The following requirements need to be described (see paragraph “D- Technical requirements”): d. Data hosting, taking account of appropriate personal data protection and data confidentiality law; e. Encryption in data exchange processes via the web interface and systems which make available files for download; f. Information Systems environments to implement; g. Data archiving; h. Performance expected from the Information System; i. Security measures to be implemented including: j. Management of data confidentiality; k. Authentication factors required; l. Transaction traceability (audit trail). Based on the context of the customer, the following requirements may also need to be detailed: m. Systems solutions favored and solutions excluded; n. Quality service level and monitoring of quality service level.	
OUTCOME	The “environment” of the registry is identified, and the technical modalities of how it shall interact with such environment (e.g. hosting, connections, security features) are specified. The Technical Specifications are completed (i.e. Stages 3 and 4) and can be shared with the selected registry providers (e.g. in the RFP) for them to submit final proposals.

3. Implementation Timeline

From start to finish, the selection of a registry provider may at least take several months up to one year. One to two additional years may be required to start operating the registry, depending on how complex the solution is, and on the level of specific IT components are required (as opposed to re-use or integrate existing software modules.)

4. An indicative list of providers of registry solutions

Table 1 below is an indicative and non-exhaustive list of suppliers of registry transaction solutions.

Table 1– Indicative list of registry services providers

Country	Supplier	Service offering	Registry Experience	References for IT systems connected to registries
Germany	LiWa GmBH	▪ Integration	▪ ETS	▪ Registry suspicious patterns detection ▪ Workflow Automation
Belgium	Trasys	▪ Integration ▪ Development	▪ ETS	▪ Central Communication Hub
China	ZBX	▪ Developer	▪ ETS	▪ Reporting platform ▪ Trading Platform
USA	SRA	▪ Development	▪ ETS	▪ NA
Japan	NTT Data	▪ Development	▪ ETS	▪ NA
United Kingdom	SFW	▪ Integration ▪ Development	▪ ETS ▪ Voluntary offset	▪ Administrative workflow automation
United Kingdom	Markit	▪ SaaS	▪ Voluntary offset	▪ Project databases ▪ Platform for initial buyer seller contact
USA	APX	▪ SaaS	▪ Voluntary offset	▪ Project databases
United Kingdom	Noumenal	▪ None	▪ Voluntary offset	▪ Project databases ▪ Communication protocol (VCSA)
France	Powernext	▪ SaaS	▪ Power sector *	▪ Hotline and administration
France	Andal Conseil	▪ Specifications / any option	▪ ETS ▪ Voluntary offset ▪ Power	▪ Registry administration ▪ Project Databases

*Examples: registries for capacity regulation, and guarantees of origin.

B- PRELIMINARY CONSIDERATIONS

1. Different registry procurement options: develop, adapt, share, or outsource

Procurement options for registries can be classified in four different categories, including:

a. **"Share"**: consists of using a single common registry. For example, the Consolidated System of European Union Registries (CSEUR) replaced all national EU ETS registries that were formerly hosted in each EU Member States and the EEA EFTA States (i.e. Norway, Iceland, and Liechtenstein), as well as the Kyoto Protocol national registries of these countries, which have their distinct obligations and connections to the UNFCCC system.[2]

b. **"Develop":** consists of drafting functional and technical specifications for an IT services provider to develop a registry system « from scratch ».

c. **"Adapt":** consists of having an IT services provider adapt and implement an existing open source registry (e.g. Open Registry) or a registry solution under license (e.g. « Greta » or « Seringas » which are under SfW license));

d. **"Software as a Service (SaaS)"**: this option is a software licensing and delivery model in which the software vendor – based on a subscription/fee – hosts and maintains the servers, databases and code that constitutes the registry application. Registry management services may also be offered (e.g. hotline, user operation management etc.). In addition to the subscription/fee, other potential costs to consider under this option include:

   - Initial specific personalization and configuration;
   - Secure hosting (e.g. annual subscription);
   - Upgrade maintenance (based on specific estimates) and upgrades imposed by [suppliers of] underlying technologies (databases etc.).

Making a decision on one of these options involves assessing them against a number of criteria such as the cost of maintenance [C], time-scale [T], know-how [S] and complexity [X], performance, security, and continuity plan [PS], flexible functionality and scalability [F], data ownership and linking [SV] and documentation and training material [D]. Table 2 compares each of the above registry procurement options to those criteria.

[2] See EU ETS Handbook available at:
http://ec.europa.eu/clima/publications/docs/ets_handbook_en.pdf

Table 2 – Comparing registry procurement options

	Advantages	Disadvantages
Share	- [C] Cost is probably low - [X] Lower level of registry complexity (implementation and maintenance) - [PS] Level of reliability and security inherited from the host system - [S] No specific requirement for technical registry expertise - [T] Operational immediately (if the registry used, does already exists) - [D] Existing documentation and training material	- [F] No possibility to implement specific functionality - [SV] To some degree lower control of data (ownership), no influence on decisions to link Market Mechanisms and subsequently to connect registries - [X] Legal issue linked to the physical location of units held - [D] Potentially a problem of Interface language
Development	- [F] Flexibility: possibility to implement specific requirements - [SV] Ownership of data and sovereignty on linking decisions	- [C] Development costs potentially higher than for other options - [PS] Risk of non-quality in a new development, including for security - [S] Expertise required in registries and Information Systems project management - [T] Takes time to implement - [D] Documentation and training material to be designed and produced
Integration	- [F] Flexibility: possibility implement specific requirements (lower than for a development from scratch) - [SV] Ownership of data and linking - [D] Existing documentation and training material can be adapted	- [S] Expertise required in registries and Information Systems project management - [T] Takes time to implement (less than for a development) - [PS] Risk of non-quality in a new development, including for security
SaaS	- [C] Cost is spread over time and predictable (contractual) - [S] No specific requirement for technical registry expertise (the basic functions exist already) - [T] Operational once the personalization and configuration project is complete. - [X] Less of a need for registry expertise and information systems project management. - [D] Existing documentation and training material which can be adapted	- [SV] Lower data ownership unless databases are hosted in the same country - [F] Little scope to respond to specific requirements, lower responsiveness to requirements for change

Some general conclusions can be drawn from the above:

- If the priority is on data ownership and sovereignty in decision making, capacity for the registry to respond to specific requirements, and ability to respond quickly to requests, then the development and integration options could be favored;

- If the priority is on reduced costs, rapid delivery, low workload and low level of internal expertise, then the use of a third-party registry (« share » option) or paying for registry as a service (SaaS) could be favored.

Note: when comparing costs it is useful to be keep in mind that any IT system generally has a limited lifespan (i.e. costs have to be compared over a time period at least equal to the lifetime of each option).

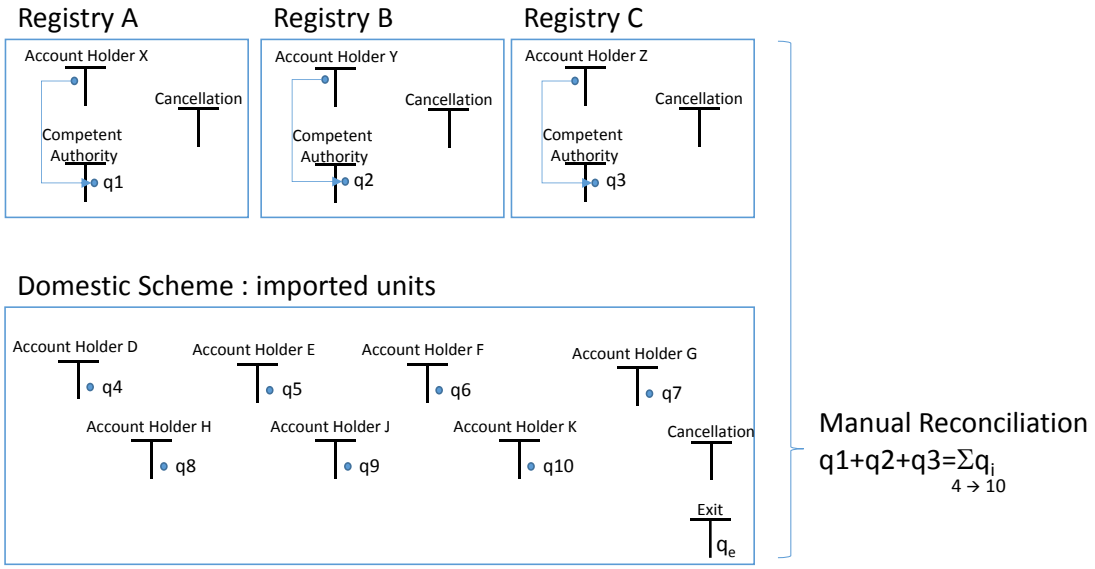
2. Accounting issues and options for import/export of units

Two main options exist for registries to ensure robust accounting when units are imported/exported from/to another registry:

- **Definitive transfer:** consists of canceling the units in the exporting registry to re-issue it in the importing registry. Such re-issuance may be done against a "proof of cancelation" generated by the exporting registry (administrator) to avoid double counting issues.

- **"Mirror" accounting:** under this option, there is no cancelation/re-issuance of the exported unit: it is stored in a special account of the exporting registry and is virtually reflected in the registry of the importing registry where it can then be subject to transfer and/or cancelation operations, as long as these are reflected in the special account in the exporting registry. For example, this is how accounting is managed for the VCS program when transfers take place between the two VCS registries: unit actually never leave the registry in which they were initially issued.

Figure 1 - Domestic chart of accounts for "Mirror accounting"



3. Registry connections

Depending on the scale of the Market Mechanism and the sophistication of the registry, a number of IT systems and databases can interface with the registry – including other registries.

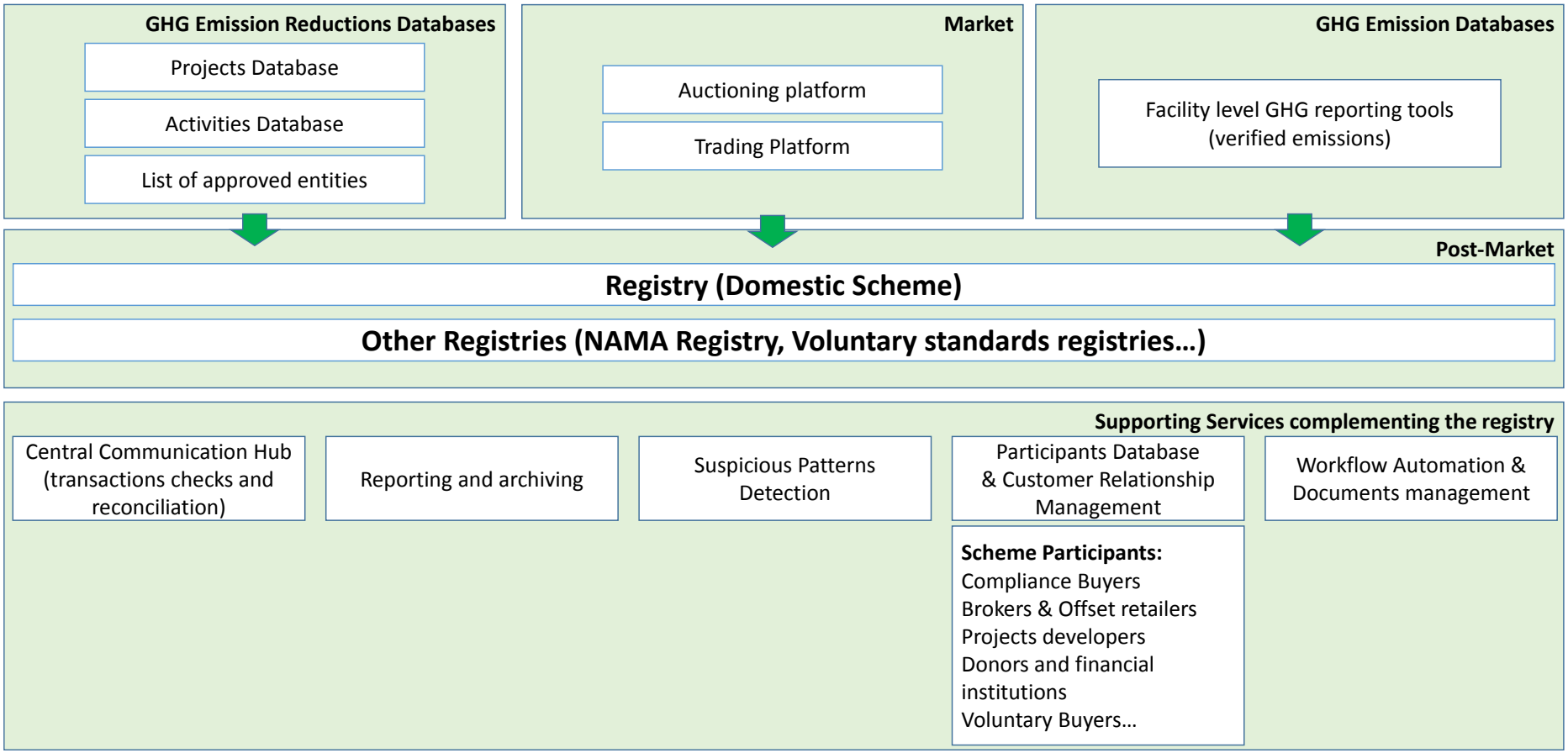
3.1. Potential IT systems and databases interfacing with a registry

Figure 2 below shows a generic functional architecture of the different IT systems which may share connections with a transaction registry:

- The upper-left box "GHG Emission Reductions Database" refers to IT Tools listing emission reduction projects or activities, and the entities approved to validate and to verify the reductions they generate.
- The "Market" box refers to IT Tools matching supply orders and demand orders (e.g. trading platform), and sending settlement instructions to the registry.
- The upper-right box "GHG Emissions Databases" refers to GHG reporting tools and platforms.
- The central part of the diagram shows the actual transaction registry, and potential other registries it may be connected to.
- The lower part of the diagram shows other systems which provide auxiliary registry services, including:

- Central communication hub;
- Reporting, logging and archiving services;
- Transaction-related and administrative events analysis services, which enable detection of suspicious behavior;
- Information database on participants in the Market Mechanism, including customer relationship management tools; and
- Automation of administrative workflow between registry administrator and account holders (e.g. account opening procedure, subsequent periodic documentation update etc.).

Figure 2 – The registry in its environment: potential connections and interfaces



3.1.1. Technical infrastructure for connection: central hub vs. peer-to-peer

The Technical infrastructure connecting distinct registries can be centralized around a communication hub (e.g. the ITL for Kyoto registries) or consists of peer-to-peer network connections.

Other type of infrastructure can also be envisaged to connect registries but may require stronger institutional and regulatory coordination:

- A single IT platform consolidating distinct registries (e.g. consolidated system of European Union registries);
- A single registry where each jurisdiction administers its own chart of accounts (issuance account, scheme participants holding accounts, cancellation accounts…).

Table 3 below lists the main advantages and disadvantages of central hub and peer-to-peer options:

Table 3 – Comparing central hubs vs. peer-to-peer architecture

	ADVANTAGES	DISADVANTAGES
Central hub	▪ Centralizes costs and complexity related to communication management and transactions controls ▪ No impact adding a new registry to the registries already connected ▪ Integrity of accounting is ensured (i.e. automatic detection of errors) ▪ Identical treatment for all transactions ▪ Imposes the same level of security for all registries; ▪ Each registry has only one connection, i.e. with the central hub ▪ Single communication protocol (e.g. UNFCCC's Data Exchange Standards).	▪ Potential sovereignty issues related to registry data made available to the entity administering the central hub administering) ▪ Costs may be high if few registries are connected ▪ Any failure of the hub paralyses the whole registry network ▪ Maintenance operations on the central hub may require a network-wide coordination
Peer-to-Peer	▪ If few registries are connected, costs may be lower	▪ Complexity and costs increase with the number of registries connected; ▪ Responsiveness to change will become challenging with the number of registries connected ▪ A security flaw in the connection between two registries poses a risk to the whole network ▪ Transactions checks may differ from one registry to the other

	▪ Network-wide reconciliation (i.e. checking for accounting consistency in all registries) is complex

From a technical, financial and security perspective, the central hub solution may be favored, especially if more than two registries are to be connected. However, issues related to technical control and sovereignty may lead to preferring a peer-to-peer architecture.

Under the Kyoto system, the ITL currently connects registries administered by different countries, developed using a range of different technologies, and connected at different points in time. Since implementation, it has overseen transfers of billions of units through hundreds of accounts. The ITL presents the following characteristics[3]:

- An architecture built around a centralized hub as opposed to peer-to-peer connections between registries;
- A standardized and secured data exchange protocol (i.e. Data Exchange Standard);
- Real-time monitoring of transactions;
- Ex-post checks: reconciliation and peer review process.

The above characteristics have allowed the ITL to offer security, reliability and credibility, operational and cost efficiency, and impartiality of treatment to the whole Kyoto registry network.

However, the EU has implemented its own central hub – i.e. the EUTL, European Union Transaction Log (EUTL. EU ETS units are transferred across EU Member States' registries through the EUTL and not through the ITL. Only transactions involving Kyoto units are checked by both the ITL and the EUTL. By doing so, the EU benefits from a central hub and ensures, while keeping that no other entity has access to EU ETS transactions and data.

3.1.2. Language for connection: communication protocols

Regardless of the above technical options chosen for connection, a communication protocol is needed for registries to be able to exchange information (e.g. UNFCCC's DES). Although the need for such "common language" may only emerge in the future, it may be anticipated in the early phases of registry development. A communication protocol imposes specific data nomenclature, value, and format for account, unit, transactions, and design of workflows

4. Registry security: issues and options

This section is dedicated to security in the design and functionality of the registry and is broken down into three parts. First, general security risk analysis questions in order to size the

[3] For more information see UNFCCC: http://unfccc.int/kyoto_protocol/registry_systems/itl/items/4065.php

required security measures, secondly the identification of the elements which may require security and lastly, a list of security functions available in the registry.

4.1. Risk assessment

Assessing risks related to the registry will pose among others the following questions: What are the risks run if a security breach occurs? Who underwrites these risks? And as a consequence, what is the acceptable cost for the security of the system?

Different types of risk need to be assessed:

- **Financial risk:** run by account holders in the case of fraud or theft of units or operational error. This risk may be proportional to the number of units held and to their market price.

- M**arket risk** and / or **reputational risk:** including the non-respect of the rules of communication of information which should have remained confidential or the communication of information which should not have been made public before a certain date. This can result for example from unintended or fraudulent modification, or disclosure of confidential data.

- **Reputational risk:** run by all participants in the Market Mechanism, by the authority in charge of the Market Mechanism and by the registry administrator in case of security failure, fraud, theft or more generally the improper use of the Market Mechanism but also in the case of operational error such as the non-respect of rules in force or simple data entry error.

These risks may incur the liability of the entity in charge of the registry administration and even the personal liability of management staff or other personnel.

A quantitative evaluation[4] of the cost of these risks enables the scoping of the security measures required (for implementation) to mitigate these risks, reduce their impact if they do occur and limit the level of financial compensation of the potentially grieved parties, as the case may be.

Note: the reputational risk may in certain cases lead to much greater costs than the cost of the units involved. For example, it may be the case for a company which communicates on its corporate social responsibility on a project which generates carbon credits. If it transpires that the credits were issued improperly due to a lack of controls by the issuing registry administrator, the company may seek compensation not just for the amount of units concerned but to the extent of damage to image incurred.

4.2. Overview of risk mitigation measures

Table 4 below proposes security measures to address these different risks.

[4] E.g. Conducting a Business Impact Assessment (BIA)

Table 4 - Security measures for different types of risks

Risk	Hierarchy of measures	Id.	Security options
Financial risk following fraud or theft of units	Mitigation	**1.**	**Terms of Use of registry services:** Require users to explicitly adhere to Terms of Use including security guidelines involving users' participation (regularly change password, use an up-to-date anti-virus etc.). **Registry functions:** Authentication, security protection for bona fide member. **IT / Technical**: See IT security measures hereafter in this report.
	Reduce impact	**2.**	**Registry functions:** Automatic alerts following detection of suspect movements and based on registry emergency service stoppages, security protection for bona fide members.
	Repair	**3.**	**Account convention:** Measures obliging the unintended receiver of units to return them. IT / Functional: The registry may require transferee's explicit acceptance of units received prior to completing any transfer.
	Compensation	**4.**	**Account convention:** Calculation rules setting a maximum value on compensation for victims, limiting the responsibility of the registry administrator.
Financial consequences, consequences for reputation or to the market following registry administrator operational errors, incorrect or premature publication of information.	Mitigation	**5.**	**Contract between the registry administrator and each user*:** explicitly indicate the list of information made public. **Awareness and training for registry administrator personnel.** **Operational procedures**: plan for monitoring and validation by a second person for sensitive operations. **Registry functions:** Rigorous management of users' authorizations (privileges). **Peer review procedures:** the main public (accounting) reports issued by the registry may be peer-reviewed by administrators of connected registries (if any) prior to publication.
	Reduce impact	**6.**	**Subscribe to an insurance policy:** associated with the operational risks of a registry administrator **Continuous improvement procedures**: integrates lessons from the experience to the operational registry administration procedures and to requirements applicable to the IT.
	Repair	7.	Ditto 3
	Compensation	8.	Ditto 4
Financial risk following user operational errors	Mitigation	**9.**	**Awareness and information of users**: via the registry web page (tutorials, video, FAQ ...) **Contract between the registry administrator and the user *:** Limit the responsibility of users Ditto 1
	Reduce impact	10.	Ditto 2
	Repair	11.	Ditto 3
	Compensation	12.	Ditto 4

Risk	Hierarchy of measures	Id.	Security options
Market; following unauthorized use of the system	Mitigation	13.	**Regulation:** Registry operations **and related banking operations** to be placed under surveillance of a market monitoring authority; facilitate the cooperation between registry administrator and any authorities carrying out police investigations; ensure that data personal protection rules do not hinder legal investigations.
	Compensation	14.	Ditto 3
Correlated subcontractor / supplier transactions	Mitigation	15.	**Demands on the entity which administers the registry:** solvency, capitalization, risk scoring, submission of audited accounts each year to the relevant authority... **Prevention of conflicts of interest**: the registry administrator (all staff included) will not hedge a position on the purchase or sale of units (outside own obligations or commitments[5]), not bring into contact buyers and sellers, not develop projects which generate credits. **Obligations of the registry administrator** to ensure that staff and contractors respect the rules of confidentiality. **Contractual clause** by which the registry administrator accepts unscheduled audits by the competent authority and carries out independent audits on a regular basis.
	Repair	16.	**Registry Administration Mandate**: build-in the possibility to terminate or bring to an end the mandate of the entity responsible for registry administration.
	Compensation	**17.**	**Registry Administration Mandate**: building an exit clause (time-scale, data transfer, knowledge transfer etc.).
Obligations of account owners or authorized representatives (users of the registry)	Mitigation	18.	**Contact:** Required documentation, document monitoring ("Know Your Customer ") and an escalation procedure in case of suspicion. More stringent requirements for market intermediaries and other voluntary participants. Regulatory instruments allowing the registry administrator to refuse the opening of an account and limiting the possibility of appeal.
	Reduce impact	19.	**Supervision of the relationship:** Supervision of daily transactions, detection of suspect behavior; reporting to the relevant authorities able to investigate or intervene.
	Repair	20.	**Terminate the relationship** Legal instruments allowing the registry administrator to refuse to open an account, to block or to close an account, to freeze or to revoke a user's access to the registry.

*: or other documents detailing the mutual obligations of the parties.

[5] E.g. buying and cancelling units for the purpose of offsetting its own GHG emissions.

4.3. IT security measures

The security of the registry system is assured by dedicated system functionalities and by technical features. Some of them are proposed hereafter.

4.3.1. Registry design

The list below proposes certain registry functions, grouped by security risk addressed.

Risk of user's identity usurpation: Verify that the person connected is the one intended by the terms of the contract and thus the one from whom documents were received and verified.

Options:

- Strength of authentication: elements that the user knows (login, password) and linked to physical items the user may have in their possession (security token or SMS code sent to mobile telephone);
- Time out: require authentication after a certain time of inactivity during which another user could use the registry on the same computer;
- Require that the password be entered again and/or an SMS code (or security token) to confirm sensitive operations.

Risk of mistaken or fraudulent transfer: Restrictions and prior warning to the risk of operational error, fraud or theft, thus protecting a good faith buyer against the risk of claims against units he holds.

Options:

- Limit access to the registry to registry administrator normal working hours;
- Checks during data entry; alerts in the case of an operation where quantities entered are greater than a certain limit or in the case of a compliance operation, entering quantities different from the regulatory obligation (example: return credits greater than or inferior to verified emissions) ;
- Workflow: operations entered by the user should be validated by another user, ensure that the beneficiary accepts liability for the quantity of units received, allow a time lapse between the validation of the operation by the transferor and notification being sent to the beneficiary during which the transferor may cancel the operation.
- "Out of band" notification (by SMS) when an operation is initiated, eventually with temporary possibility to cancel it;
- Implement a pre-entered list of beneficiaries associated with an account to mitigate the risk of incorrect entry of a beneficiary account number and to mitigate the risk of theft of units.

Risk of mistaken or fraudulent operations: Permit incorrect operations to be corrected; emergency stops and quarantine functions

Options:

- Allow for limited delay between the last stage of validation of an operation by the transferor and completing the transfer, during which time an operation can be cancelled through an emergency procedure;
- Enable the registry with emergency stop functions, revoke users, block accounts, reverse operations;

Risk of suspicious activity: detect and alert to suspect behavior

Options:

- Develop detection and alert functions to detect suspicious administrative events (e.g. frequency of change of authorized registry users) or suspicious transactions (e.g. where the same unit serial numbers are exchanged in high numbers, at unusual frequency or volume);
- Repeated transfers between counterparts ruled by different fiscal buy / sell regulations (e.g. buying without VAT (offshore or reverse-charge) and selling with VAT).

Risk related to significant changes in the risk-profile of account holders: Ensure systematic and up-to-date checks on documents produced by users

Options:

- Develop customer relationship management functions with alerts in the case of obsolete documents or checks not done;
- Computerize the administrative workflow of initial contact and customer relationship management;
- Computerize the risk-profiling of users;
- Subscription to external databases of company information, companies' owners and managers.

4.3.2. IT security

The "Data Exchange Standards" (DES) standard published by UNFCCC describes a set of security measures for registry information systems. Certain measures are generic, others relate specifically to the connection between a registry and a central hub.

Below is a list of the main Information Systems Security requirements for registries independent of their connection to a central hub such as ITL according to DES version December 2013:

Table 5 - List of the main Information Systems Security requirements for registries

Paragraph	Security measures
3.1.1	Registry Systems have fixed public IP addresses
3.1.3	The use of SSL will protect any communications that may pass over the networks at the registry site
3.1.4	Use of a trusted Certificate Authority
9.	Documentation to show that (…) the registry will be operated in a manner consistent with excellent operating practices. These requirements ensure the registry has an adequate plan for addressing operational and security requirements of the application
9.1.1	Database and Application Backup
9.1.2	Disaster Recovery Plan
9.1.3	Security Plan
9.1.4	Application Logging Documentation
9.1.5	Time Validation Plan
9.1.6	Version Change Management
9.1.7	Test Plan and Test Report
9.1.8	Operational Plan

In addition, if the context requires it (e.g. financial gain resulting from identity theft of the registry administrator) several options may contribute to mitigate the risk of registry administrator's identity usurpation:

- Dedicated machine, without Internet access except for a dedicated URL required for administration of the registry;
- Dedicated machine with fixed IP which is recognized by the registry system;
- Dedicated machine with no peripherals;
- Impossibility to connect as registry administrator via the URL used by other users;
- Strong authentication: login, password and token-key;
- Physical access security: office badge access required, security-guarded premises outside working hours.

Other IT security measures are described in the Technical Specifications (see paragraph "Security requirements" hereafter in this document).

C- FUNCTIONAL SPECIFICATIONS

1. Defining the data to be managed by the registry

1.1. Overview of user related data

The registry administrator establishes a relation (eventually a contract) with the account holder who is in general and preferably[6] a company rather than a natural person. The account holder designates Natural Persons as "authorized representatives".

Each account belongs to one and only one account holder. At least two persons may be authorized to enter and validates transactions on this account (the "authorized representatives").

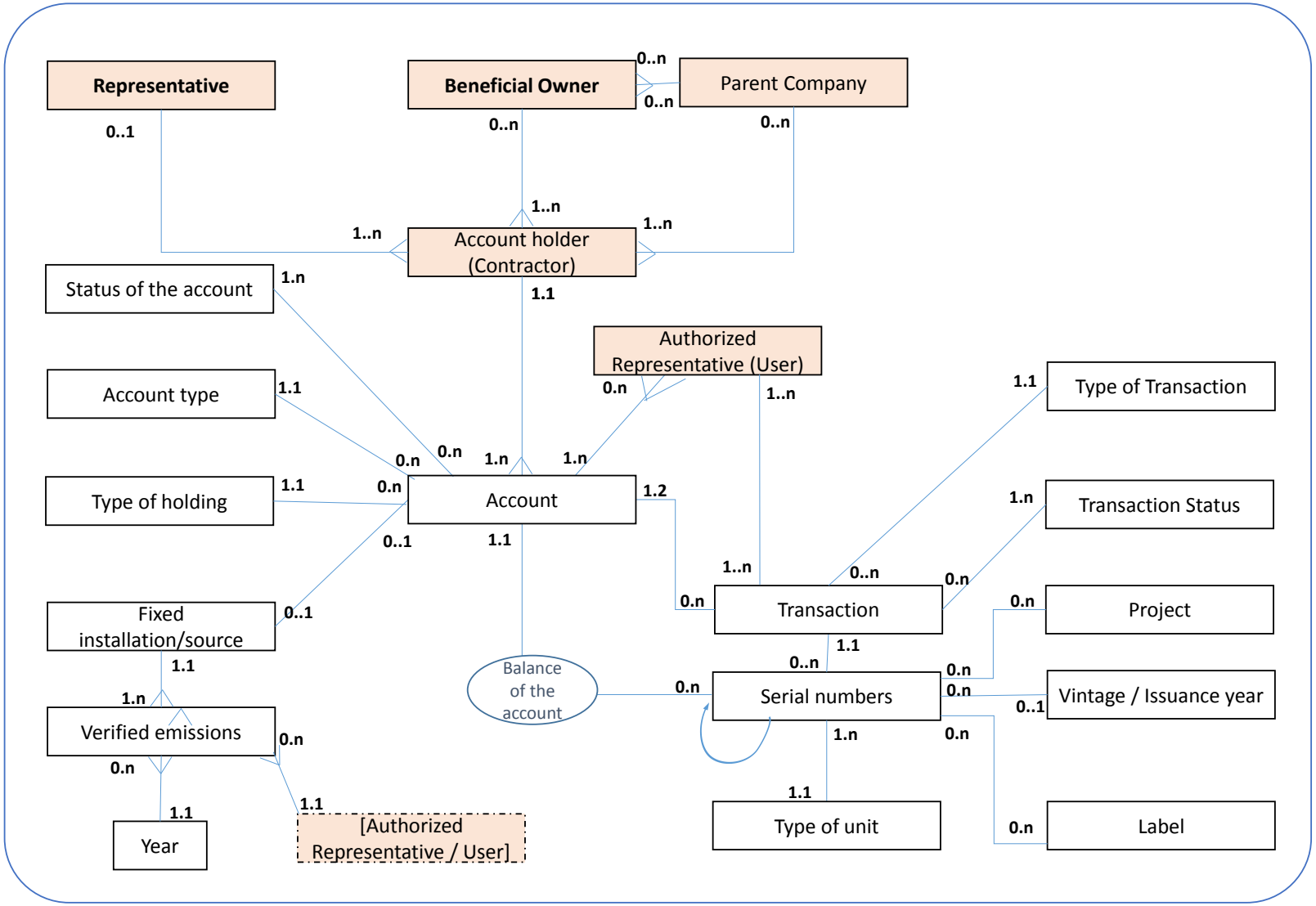
In order to properly monitor risks, to carry out the checks required by regulations including those related to money-laundering and terrorism financing, it is necessary to identify the "beneficial owners[7]" i.e. Natural Persons who effectively benefit from the company transaction (majority shareholder for example).

Figure 3 below represents the relationships between these data.

[6] A company can be checked for its liability through mandatory and public documents.

[7] FATF (Financial Action Task Force) definition: "Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted." It also includes those persons who exercise ultimate effective control over a legal person or arrangement. (…)"

Figure 3 - Entity relationship diagram[8]



[8] Data related to users (account holder and account representatives) are colored in pink.

1.1.1. Focus on the beneficial owner

The question of "beneficial owner is covered by the FATF [9] recommendations (R24 and R25) and respective explanatory notes available on the FATF site.

The measures proposed here to protect the greenhouse gas emissions market mechanism from being used for money laundering or to finance terrorism is to insist on transparency regarding the Natural Persons who benefit from transactions initiated by account holders.

The outcome expected is to detect fraudulent use likely to be hiding behind one or more front organizations.

In order to do so the registry administrator will request, that Natural Persons who are the "beneficial owners" of companies holding accounts in the registry be identified. Similarly, the registry administrator may request that beneficial owners of transactions carried out for on behalf of third parties be identified.

Over and above information requested on initial account opening and documentation renewal, it is also recommended to distinguish accounts used for the account holder (the beneficiary of the account is the same as the account holder) from accounts opened for third parties.

1.1.2. User authorization profiles

Not all data is public or accessible to all authenticated users. Similarly all functions are not available to authenticate users.

The following user authorization profiles (i.e. “user profile”) are proposed for the different types of Natural Person registry users. A summary description of the level of authorization is to be found in this table, however to configure the registry, it is necessary to detail whether a user profile has access to a function or not (see the proposed list of functions and related authorizations annexed to this document).

Table 6: Proposed list of user authorization profiles

User authorization profile	Data access	Access to functions
Information system administrator	All	All
Registry administrator	All	All
Registry operator	All	All except validation
Authorized representative	Designated holder accounts and transactions on these accounts	Entering transfers and cancellations
Additional authorized representative		Validation of transfers and cancellations
Account auditor		Read only

[9] Financial Action Task Force: organization created in 1989 with the objective of developing and promoting policies against money-laundering and the financing of terrorism.

Sole representative[10]		Entering and validation of transfers and cancellations
Any user	Public reports	Read only.

1.2. Chart of accounts and accounting models

1.2.1. Chart of accounts

The registry administrator must establish a list of accounts distinguishing various "account types" required by the Market Mechanism.

The diagram below illustrates an indicative chart of accounts which implements various types of accounts such as cancellation accounts, holding and buffer accounts etc.

Note: The black circle marked "-Q" represents the structurally in-debit technical account which is debited in quantity (without serial number) on each issuance. Indeed, a registry uses double entry book-keeping (a generally agreed accounting principle): any unit credited to an account (including at issuance) must have a counterpart debit on another account.

The different types of accounts proposed are:

Technical accounts managed by the authority in charge of the Market Mechanism (or the Regulator):

- The **issuance account** (and its counterpart the "-Q" account) will receive units issued, before transferring them to a client's holding account;
- The **surrendering account** is used in the case of an ETS, to receive units surrendered by liable parties in the same quantity as their verified emissions;
- A **deletion account** and a **cancellation account. T**his distinction enables the following: following an operational error for example an over issuance, units will be transferred to the deletion account whereas units cancelled to comply with the Market Mechanism regulation, will be transferred on the cancellation account;
- The **risk buffer** account: dedicated to manage risk through buffered units;
- The **exit account**: this technical account is credited for any unit leaving the registry. This allows the registry to function using double-entry book keeping (the debit of an account transferring units to another registry is balanced by the credit to this technical account).

Holding accounts required for scheme participants:

- The auction delivery account: if the authority in charge of the Market Mechanism sells units ;

[10] The case of an account holder who may not designate more than one person to manage their registry account.

- National/Jurisdictional Holding Account: if the Market Mechanism is established at national/jurisdictional level and requires National/Jurisdictional holding of units;
- Trading Platform Account: required depending whether there is a trading platform in place and depending on how trades are to be settled within the registry (directly on market participants accounts vs. on the trading platform account, ensuring opaque counterparts, and to be followed by an end of day net clearing among participants registry accounts);;
- Operator Holding Account: for persons required or encouraged to adhere to the Market Mechanism;
- Project Proponent Holding Account: for Project Developers receiving credits issued based on project verification reports.

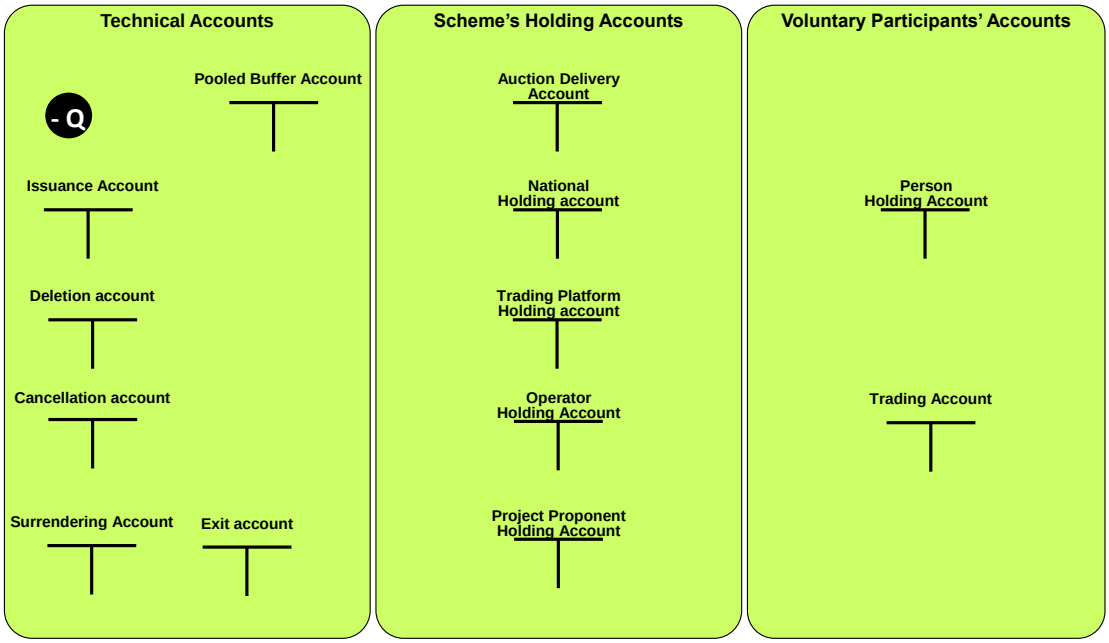
Holding accounts for those who participate voluntarily in the system intermediaries, etc.):

- Natural Person Holding Account: accounts for Natural Persons as required;
- Trading account: especially for brokers and other market intermediaries.

Notes:

- Holders of operator accounts may also wish to open a trading account;
- It may be necessary to determine whether appropriate to allow accounts to be opened for Natural Persons in a relatively complex and financially risky mechanism due to the difficulty to make sure that such natural persons are fully aware of the rules and risks related to trading, and also due to the difficulty for the registry administrator to assess the reliability of a Natural Person (as compared to the ways and means available to assess the reliability of a legal entity with public records).

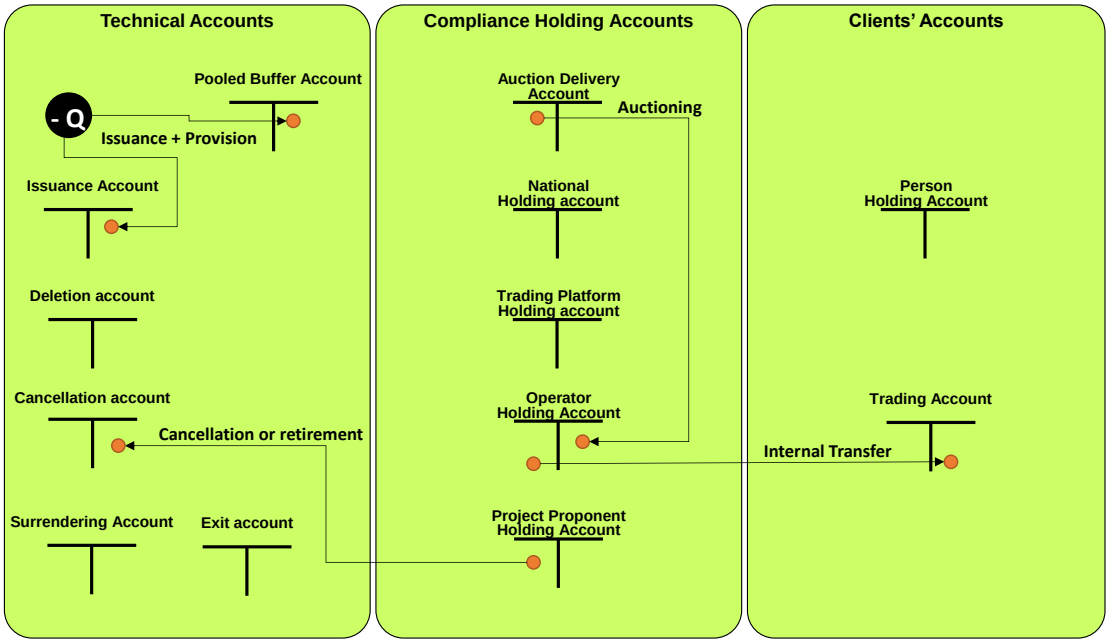
Figure 4 - Indicative chart of accounts for a registry



1.2.2. Accounting models

To follow, for the above chart of accounts, are detailed the accounting models for the main types of transactions which a registry must manage (excluding transfers between registries): issuances, buffers and buffer release, internal transfers, cancellations. The accounting models described hereafter comply with the transactions workflow described in this document.

Figure 5 – Accounting models for key transactions



Each transaction within the registry will debit an account and credit another account. Restrictions on account type debited or credited by each transaction type can be implemented. The table below details for each type of transaction, the accounts eligible for debit and credit.

Table 7 - Accounting models: type of accounts debited or credited by type of transaction

Type of account	Type of holding	Account holder	Type of transaction													
			Provisioning		**Buffer release**		Issuance		**Transfer**		Surrender		**Technical deletion**		Withdrawal	
			DB	CR	**DB**	**CR**	DB	CR	**DB**	**CR**	DB	CR	**DB**	**CR**	DB	CR
« -Q »	Proprietary	CE/S[11]	Yes				Yes									
Issuance	Proprietary	CE/S						Yes					**Yes**			
User	Proprietary	Customer						Yes	Yes	Yes	Yes		**Yes**			
Project proponent	Proprietary	Customer				Yes		Yes	Yes	Yes			**Yes**			
Buffer	Third-party	CE/S		Yes	Yes			Yes								
Other holding[12]	All	Customer							Yes	Yes			**Yes**			
Return	Third-party	CE/S										Yes			Yes	
Withdrawal	Proprietary	CE/S														Yes
Cancellation	Third-party	CE/S	**XX**[13]		**XX**	Yes	**XX**		**XX**		**XX**		**XX**			
Deletion	Proprietary	CE/S	**XX**		**XX**		**XX**		**XX**		**XX**		**XX**	**Yes**		

[11] CE/S: Competent authority or State

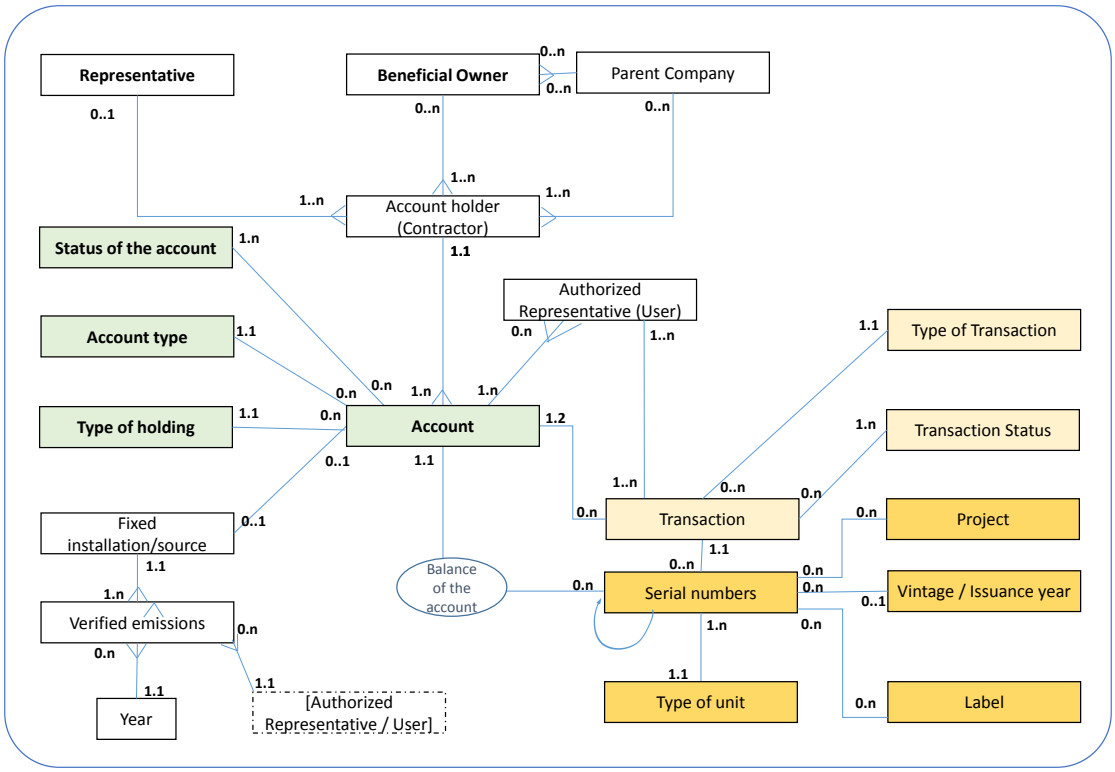
[12] Trading account, personal holding account, ...

[13] XX: Debit is not permitted on this account for any transaction

1.3. Overview of data related to accounts and units

Figure 6 - Conceptual data modelFigure 6 below is an indicative conceptual data model (with focus set on units i.e. serial numbers).

Figure 6 - Conceptual data model



The figure above shows data related to accounts in green, transactions in light-orange and units in dark orange.

The type of holding

The type of holding can take two values: holding for own use (proprietary trading) or holding for a third party.

In the case of a unit held for own use, the account holder declares being the beneficial owner of any transaction on the account.

Where an account is held for a third party or to trade on behalf of third parties, the account holder declares that all transactions are carried out for on the behalf of a third party ”beneficial owner”.

Purpose of the recursive relationship on the "Serial numbers" entity.

Serial numbers are managed by blocks of consecutive numbers (example: the block 501-1500 is a block made up of 1000 similar units, of the same type, label, vintage and project).

However a transaction can break this block up. This is the case if a block of 500 units is to be debited from the account which holds the block.

Table 8 - Management of blocks of serial numbers (hypothesis: LIFO)

	Transferor account		Account of the beneficiary	
	Debit	**Credit**	**Debit**	**Credit**
Block of serial numbers before transfer		501-**1500**		
Accounting model of a transfer of 500 units	500 →			→500
Account balance after transfer		501-**1000**		**1001.-1500**

T / P / L / t = characteristics of the unit, T (type), P (Project), L (Label), t (validity period or

The recursive relationship represents the fact that the registry conserves the history of breakup of blocks of serial numbers. This allows an audit or in the case of a reconciliation error to trace a serial number back to its original "block".

Label

The label represents a quality certificate that could be associated with a serial number. CCBA[14] or Social Carbon are examples of labels that can be borne by carbon credits.

FIFO, LIFO or "undetermined"

Technically, when a transaction debits an account within a range of serial numbers, the registry must select serial numbers to take from the block of available serial numbers.

Several options are possible

- LIFO: Last in First Out. The serial numbers to be debited first are the latest, by date, to have been added to the account. To choose between serial numbers credited on the same date, a second criteria is required (for example serial number);
- FIFO: First In First Out. The serial numbers to be debited first are those which were first added to the account by date. To choose between serial numbers credited on the same date, a second criteria is required (for example serial number);
- User's choice: the user chooses the serial numbers for the transaction. The user can select a rule (FIFO or LIFO) or even choose individual serial numbers.

Note: the registry allows the user entering a transaction, to select a given project, a given label, a specific vintage or year of issuance associated with the units involved by the transaction (transfer, cancellation, etc.).. The FIFO / LIFO rule then applies.

1.4. Standardized nomenclatures and values

[14] The Climate, Community & Biodiversity Alliance

With the aim in mind of connecting together registries in the future, it is recommended to adhere from start to the nomenclatures and value lists of the Data Exchange Standard, as per annexes F and G in the November 2013 version.

Note: In avoidance of any doubt, adhering to the DES will make it easier for registries to connect, without any commitment to ever connect to the ITL.

Illustrations: the DES reserves values

- 1 to 7 for unit types within the (scope of) the Kyoto protocol; values from 8 onwards are therefore available to manage other types of unit;
- 100 for "Holding Account" account type and 250 for "Voluntary Cancellation Account" account type.

The table below lists the main nomenclature and codes which are standardized by the DES.

Table 9 – List of nomenclatures and codes reserved by the DES

Reference to the DES	Code	DES Reserved values
Annex G Fig. 1	Type of account	Discrete values between 100 and 423
Annex G Fig. 3	Guarantee period	0 to 4
Annex G Fig. 4	UTCF/LULUCF activity	1 to 7
Annex G Fig. 5	Notification status	1 to 3
Annex G Fig. 6	Type of notification	1 to 11
Annex G Fig. 7	Participant status	1 ; 2
Annex G Fig. 8	Reconciliation status	0 to 11 ; 98 ; 99
Annex G Fig. 9	Transaction status	1 to 16
Annex G Fig.10	Transaction type	1 to 10
Annex G Fig.11	Type of unit:	1 to 7

2. Transactions to be Managed by a Registry

The life cycle of a unit is very often determined by three main stages:

- It's creation (issuance);
- Change of ownership (allocation, auction, transfer) or even intermediate transformation (adding a label, conversion ...); and
- End of life (cancellation, surrendering, deletion...).

The registry offers different transactions to account (and to keep records) for each of these stages, serial number by serial number.

To follow is a description of the main transactions that a registry must be able to execute and account for: a workflow is suggested as well as a chart of accounts and a diagram of status changes.

Specific requirements of each Market Mechanism may lead to specify other types of transaction and/or alternate workflows, which can be performed by cloning and adaptation of those suggested below.

2.1. Issuance without provision for risk

Units are issued in accordance with applicable rules and under the responsibility of the registry administrator. Examples are: issuance of quotas in accordance with commitment to cap greenhouse gases emissions; issuance of credits in accordance with the procedure in force and consistently with the project's verification reports.

2.1.1. Accounting for unit issuance

Issuances initiating event may be a manual instruction (for example receiving a verification report for a project) or an imported file handled automatically (for example for an ETS, the validation of an "allocation table" which determines, for each participant in the market, the amount of quota each will receive).

The registry will credit the units on the beneficiary account unless its status precludes doing so (account blocked or closed).

- At issuance, the units are created in the registry with a unique serial number;
- In the case of credits issuance:
  - A permanent link associates each unit created with the initiating project. This link is created by combining the project identifier and the units' serial numbers;
  - A quality label (CCBA, Social Carbon ...) may be associated with the units issued;
- The unit may be associated with a specific period: vintage of emission reductions under the VCS standard, year of issuance of credits under the Clean Development Mechanism, commitment period limiting the use of units for compliance purpose under the Kyoto Protocol;
- The registry automatically notifies the authorized account users associated with the beneficiary account.

The table below represents the accounting model for an issuance

Table 10 - Issuance accounting model

	"-Q" Account		**Beneficiary account**	
	Debit	**Credit**	**Debit**	**Credit**
Account balance before transfer				Quantity Q2 T / P / L / t
Accounting model for issuance of "q" units of type "T"	Quantity: **q** →			Quantity: **q**
Account balance after transfer				Quantity: Q2+**q** T / P / L / t

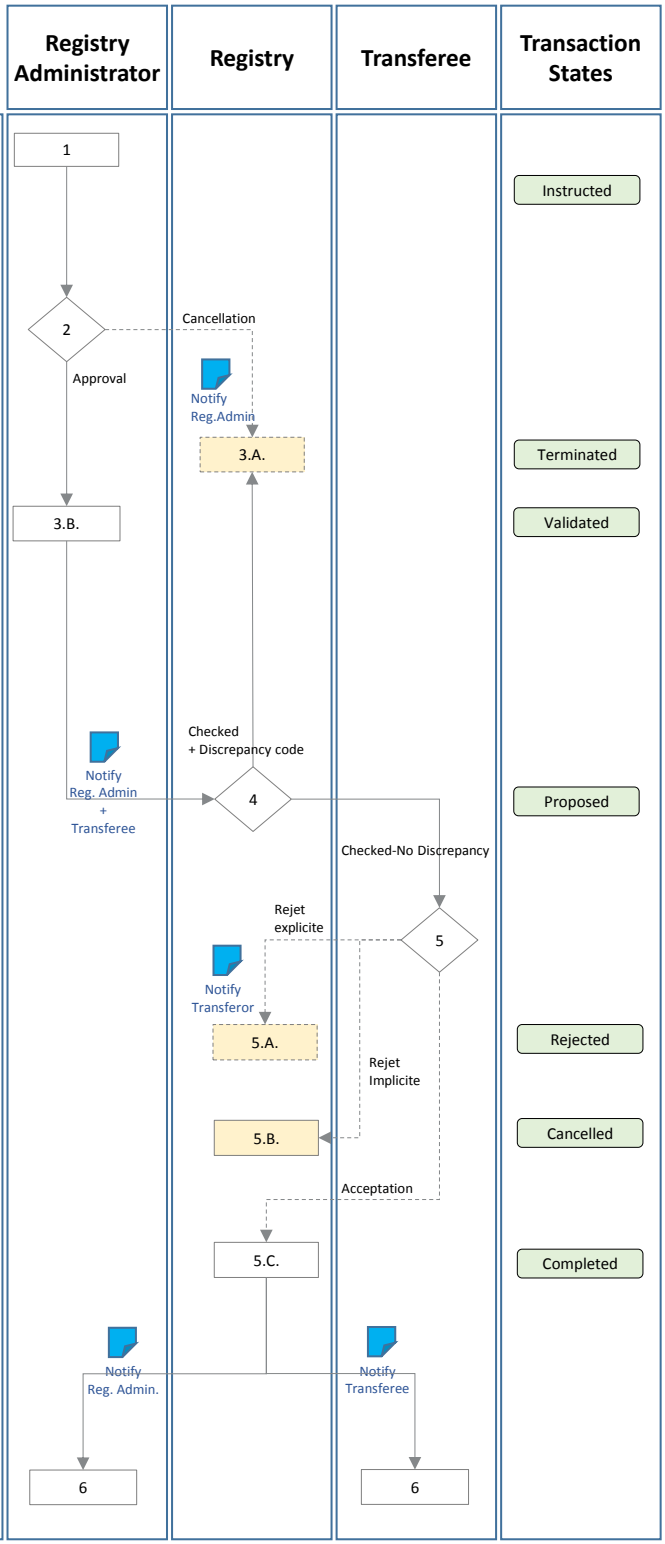
T / P / L / t = characteristics of the unit, T (type), P (Project), L (Label), t (validity period or vintage).

Figure 7 – Issuance: Proposed workflow diagram

1. The administrator of the registry is responsible for the issuance: he authorizes it as necessary by approving an integrated file. The date of the transaction is automatically set to the current date. Serial numbers are created.
2. Four-eye principle (optional): the issuance is monitored by a user different from the one who authorized it.
3. A. – The issuance is cancelled.
3. B. – The issuance is approved.
Depending on optional security options, approval may require a password or code sent by SMS to be entered.
Approval of the issuance is notified to authorized representatives of the transferee account.
4. – If applicable, the issuance is proposed to the central hub which carries out checks. The registry receives a response from the platform. If there is no discrepancy, the transfer may be finalized, otherwise it is cancelled.
5.Option: explicit approval may be required for the issuance from one of the authorized representatives of the transferee account.
5.A – In the case of an explicit rejection, the system cancels the issuance.

5.B – Option: an issuance may be cancelled automatically after a specific time lapse without explicit approval.
5.C. – The issuance is accepted (explicitly or implicitly according to the design of the system). The transferee account inventory is updated.

6. The registry produces notifications of issuance which can be downloaded on-line. The administrator of the registry and authorized representatives of the transferee account are notified.

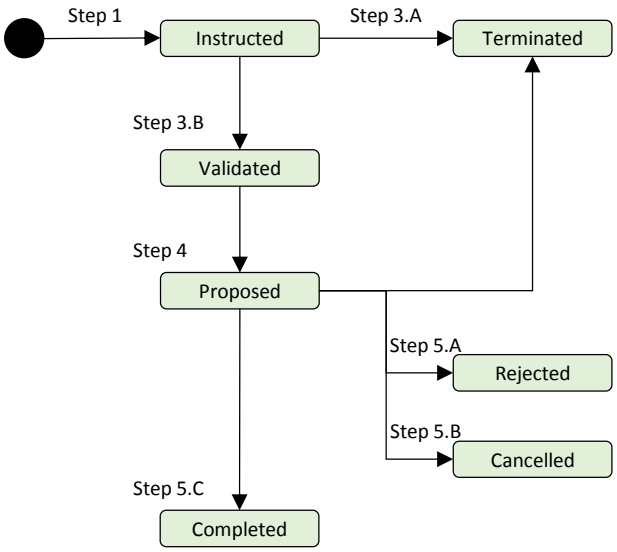


2.1.2. Issuance statuses and status changes

The registry keeps an audit trail of statuses and status changes of all issuances.

The diagram below shows the changes in status for an issuance according to the workflow proposed above.

Figure 8 - Issuance – transaction status and status changes.



2.1.3. Options and variants

1. Security measures related to the instruction of an issuance

The issuance is under the responsibility of the registry administrator. Therefore, the workflow above assumes that it is not necessary to provide the same level of security and cancellation period as for transfers, but other choices are possible. Notably the same workflow and time-scale may apply to all transactions, issuances included.

Similarly the requirements for confirmation of a password or data entry by SMS is a security option which is supposed here unnecessary to impose on registry administration staff.

An alternative to these security measures consists of a "6-eye" checking system (a third user over and above the two first would also check the issuance).

2. Measures to ensure the responsibility of the beneficiary

The registry can automatically notify the beneficiaries of an issuance. This notification can be delivered by e-mail or "out of band" via SMS for additional security.

Explicit validation may be required by the beneficiary. After a certain time lapse, an issuance not explicitly validated by the beneficiary can be automatically validated (or rejected, but the risk is that the registry administrator may have to re-enter issuances).

These non-exclusive measures ensure that the beneficiary takes responsibility for the reception of units issued in his favor and reduces the adverse consequences of operational error.

2.2. Issuance with risk buffer

Certain standards manage the risk of non-permanent emissions reductions in agricultural and forestry sectors (of which REDD+) by withholding credits on a dedicated account.

At each issuance, up to 3 operations may need to be accounted for:

- The units issued to the project proponent;
- The units issued to a risk buffer account. The buffer account may be common to all projects or one managed specifically for a set of projects, for a sector or for a country/jurisdiction;
- Under certain conditions, a release of buffer units buffered at former issuances, to be accounted for as a credits to the project proponent's account.

The verification report provides the quantities concerned for each operation:

- "q" is the quantity to credit to the beneficiary account;
- "b" is the quantity to buffer; and
- "r" is the quantity to release from the buffer account and to credit to the beneficiary account (r can be zero).

The greenhouse gas emissions avoided / sequestered during the verification period triggering the issuance, amount to "q + b" tons of CO2 eq.

The registry creates a link between these operations. All of these operations link to the same project and to the same verification report, and all credits and debits to the buffer account are linked to the issuance.

2.2.1. Issuance of “q” units credited to the project proponent account

The accounting model and workflow for issuance of credits are identical to those described above for issuance transactions without risk buffer.

2.2.2. Issuance of “b” buffer credits to a risk buffer accounts

The table below represents the accounting model for “crediting” a risk buffer account. The transaction is very similar to an issuance, crediting a "technical" (risk buffer) account.

Table 11 - Accounting for unit buffers

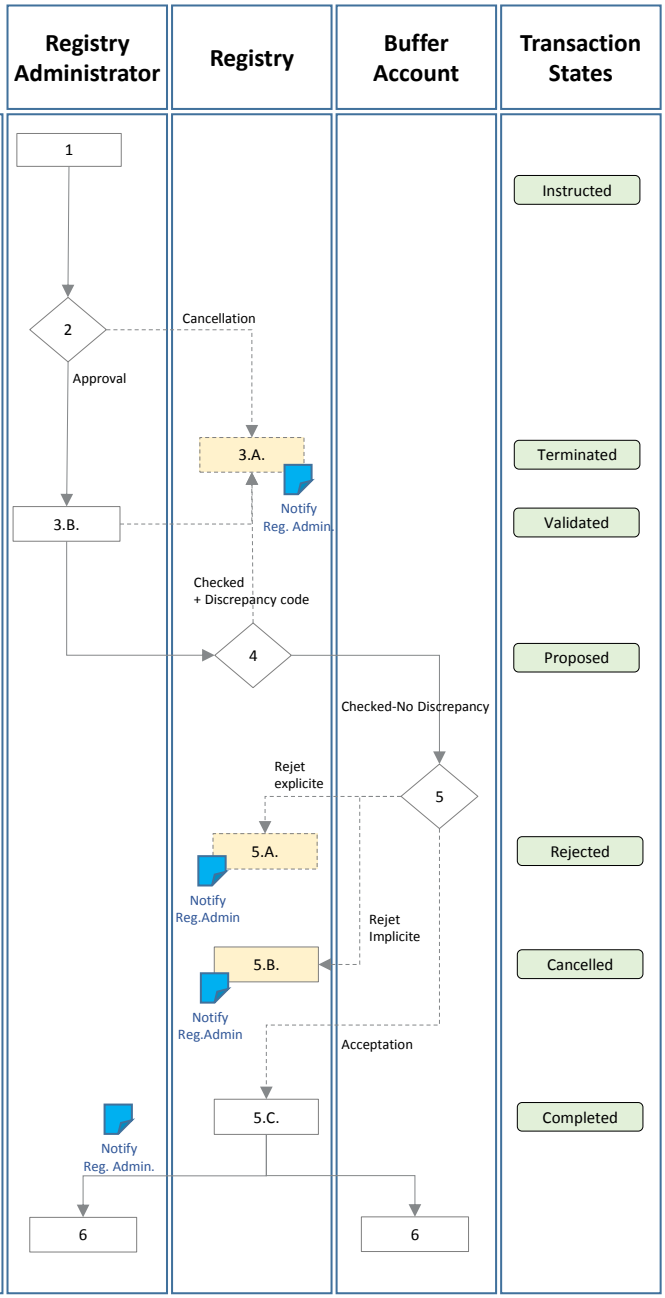
	"-Q" Account		Buffer account	
	Debit	**Credit**	**Debit**	**Credit**
Account balance before transfer				Quantity Q2 T / P / L / t
Accounting model for issuance of "q" units of type "T"	Quantity: **q** →			→ Quantity: **q**
Account balance after transfer				Quantity: Q2+**q** T / P / L / t

T / P / L / t = characteristics of the unit, T (type), P (Project), L (Label), t (validity period or vintage).

The diagram below represents the workflow crediting a risk buffer account.

Figure 9 – Issuance with buffer credits: Proposed workflow diagram

1. The administrator authorizes the issuance. The date of the transaction is automatically set to the current date.
2. Four-eye principle (optional): the issuance is monitored by a user different from the one who authorized it.
3. A. – The issuance is cancelled.
3. B. – The issuance is approved. Depending on optional security options, approval may require a password or code sent by SMS to be entered. Serial numbers are created. Options: The transaction can be cancelled (delay before completion, or request to enter a SMS code or password following incorrect entry)
4. – If applicable, the issuance is proposed to the central hub which carries out checks. If there is no discrepancy, the transfer may be finalized, otherwise it is cancelled.
5.Option: explicit approval may be required for the issuance from one of the authorized representatives of the transferee account.
5.A – In the case of an explicit rejection, the system cancels the issuance.
5.B – Option: an issuance may be cancelled automatically after a specific time lapse without explicit approval.
5.C. – The issuance is accepted (explicitly or implicitly according to the design of the system). The transferee account inventory is updated.
6. The registry produces notifications of issuance which can be downloaded on-line. The administrator of the registry is notified.

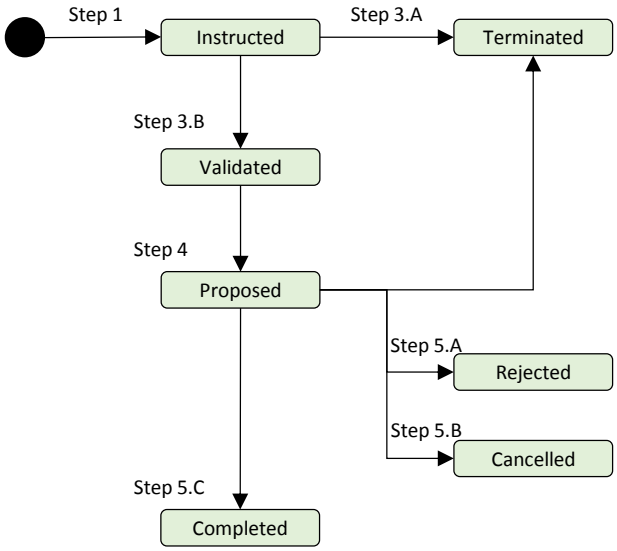


2.2.1. Transaction statuses and transaction status changes

The registry keeps in the audit trail the history of the statuses and status changes of each transaction.

The diagram below shows these status changes in the case of an issuance of buffer credit as per the workflow presented above.

Figure 10 - Issuance of buffer credits – transaction statuses and status changes



2.2.1. Release of "r" buffer credits

The risk buffer release transaction is an internal transfer, initiated by the registry administrator debiting the buffer account and crediting the project proponent account. The workflow is that of an internal transfer. The accounting model is as follows:

Figure 11 - Accounting for risk buffer release

	Buffer account		**Beneficiary account**	
	Debit	**Credit**	**Debit**	**Credit**
Account balance before transfer		Quantity: Q1		Quantity Q2 T / P / L / t
Accounting model: release of risk buffer of "r" units	Quantity **r**	→	→	Quantity **r**
Account balance after transfer		Quantity: Q1-r		Quantity: Q2+r (unchanged) T / P / L / t

T / P / L / t = characteristics of the unit, T (type), P (Project), L (Label), t (validity period or vintage).

2.3. Allocation

Allocation is specific to ETS: this operation transfers entitlements to emit GHG to a list of entities (installations) committed to comply with the ETS in place.

Therefore, allocation will occur after issuance and consists, in fact, in a « batch » of internal transfers debiting the account of the authority in charge of the Market Mechanism (or the regulator) and crediting installations.

Handling manually with allocation may be an issue if there are a lot of installations to be credited in a limited time-window. In order to deal with such a situation:

- The registry will propose a dedicated function, allocating units based on an imported "allocation table";
- Allocation will be accounted immediately, without requesting beneficiaries to explicitly accept allocated units and thus reducing the risk of rejection.

2.4. Internal transfers

2.4.1. Accounting for internal Transfers

Internal transfers involve two account holders: the transferor and the transferee. Upon request by the transferor, the registry transfers a certain quantity of units from its account to that of the transferee, unless the account status of the transferor or the account status of the transferee is incompatible with such transfer.

In accounting terms, an internal transfer subtracts a certain quantity of units from the inventory of the transferor's account to add the same quantity to the inventory of the transferee's account. The transferred units retain their unique serial number, and the registry automatically notifies authorized users linked to both accounts.

The table below shows the accounting model of an internal transfer.

Table 12 - Accounting for internal transfers

	Transferor's account		Transferee's account	
	Debit	**Credit**	**Debit**	**Credit**
Inventory of the account before the transfer		Quantity: Q1 Unit type: T		Quantity: Q2 Unit type: T
Accounting scheme for the transfer of "q" units of "T" type	Quantity: **q** Unit type: T Serial numbers: from x to y	→	→	Quantity: **q** Unit type: T Serial numbers: from x to y
Inventory of the account after the transfer		Quantity: Q1-**q** Unit type: T		Quantity: Q2+**q** Unit type: T

T / P / L / t = characteristics of the unit, T (type), P (Project), L (Label), t (validity period or vintage)

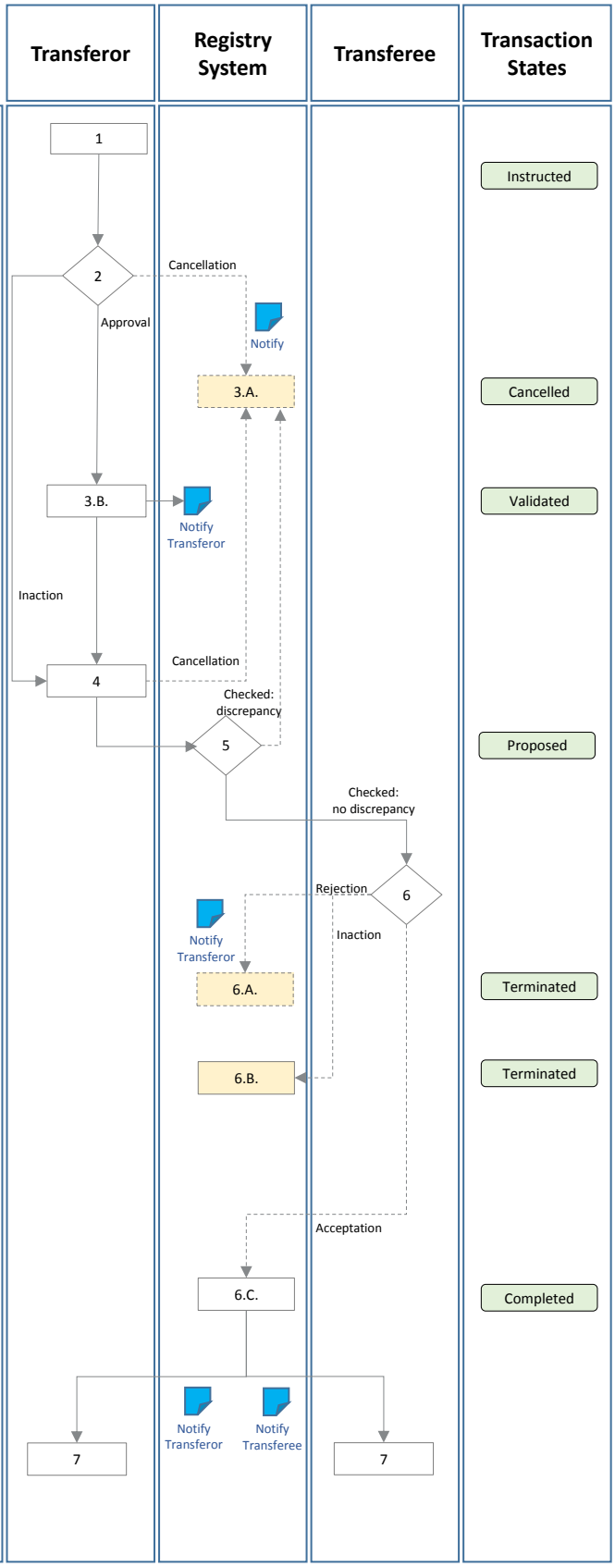
The diagram below proposes a workflow for internal transfers. Optional security measures proposed and their variants are then discussed.

Figure 12 - Internal transfer: Proposed workflow diagram

1. An authorized representative instructs the transfer to debit the transferor's account. The date of the transaction is automatically set to the current date.
2. Four-eye principle (optional): the transfer is reviewed by an authorized representative different from the one who instructed the transfer.
3. A. - The transfer is cancelled.
3. B. - The transfer is approved. (Based on optional security measures, such approval may require entering a password or an SMS code). The serial numbers affected by this transaction are no longer available for any transaction.

4. Option: after a certain time, an automatic decision may cancel or confirm the transfer.
5. If applicable, transfer to the central hub for a check (e.g. internal transfer between accounts bearing distinct account types).

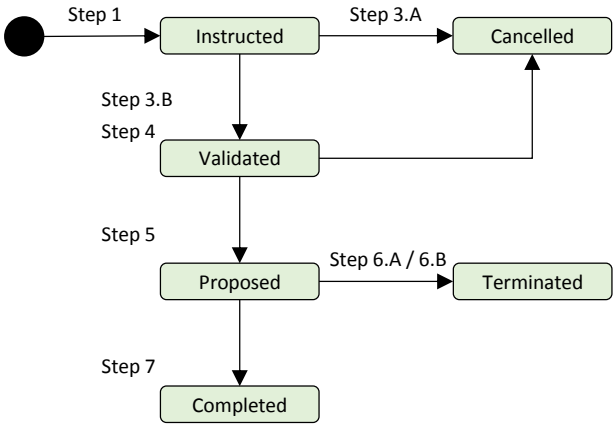
6. Option: explicit approval of the transfer may be required by one of the authorized representatives of the transferee's account.
6.A - In case of rejection of the transfer by the transferee, the system cancels the transaction and restores the inventory of the transferor's account to its position prior to the transfer.
6.B – Option: the rejection of the transfer can be performed automatically after a certain period without explicit approval by an authorized representative of the transferee's account.
6.C. - The transfer is approved (either explicitly or automatically depending on the system design). The inventories of the accounts involved in the transfer are updated.
7. The registry produces transfer notifications that are downloadable online. The authorized representatives of the transferor's account and the transferee's account are both notified.



2.4.2. Transaction statuses and transaction status changes

The registry keeps in the audit trail the history of the statuses and status changes of each transaction. The diagram below shows these status changes in the case of an internal transfer as per the workflow proposed above.

Figure 13 - Internal transfer – transaction statuses and status changes



2.4.3. Options and variants

Transferor's security and accountability measures

Prior to debiting the transferor's account, various security measures may be considered to limit the risk of mistaken or fraudulent transfers.

These can range from an "out of band" notification (by sending a SMS) to the requirement of an explicit confirmation (reentering user's password, approval by an authorized representative other than the one who instructed the internal transfer (4 eye principle) or entry of a confirmation code from a security token or sent automatically by the registry by SMS to one of the authorized representatives associated with the transferor's account).

Other options prior to notifying the transferee:

- Automatic cancellation of any internal transfer entered and not approved after a defined time lapse;
- Cancellation period offered to the transferor's authorized representatives.
- Transferee's accountability measures:
    - The registry may automatically notify the transferee of any internal transfer credited to one of its accounts. These notifications can be issued by email, or "out of band" via SMS for enhanced security.
    - An explicit approval by the transferee may also be required for any transfer. After a certain time lapse, a transfer received and not expressly approved by the transferee may be automatically approved or rejected, depending on the design chosen by the designers of the registry's computer system.

These measures, which are not mutually exclusive, do not only serve to enhance system security. They explicitly commit the responsibility of the transferor and the beneficiary in recognition of internal transfer and thereby protect "good faith buyers" against the risk of being claimed for units they hold.

2.5. External transfers

An external transfer is an operation initiated by the transferor to transfer units to a third party (the transferee) whose account is held in another registry. In the simplest case, both accounts are open and the transfer is accounted for. However at the time of the transfer is initiated, the transferring registry has no knowledge of the existence, or the status, of the transferee's account in the receiving registry. A dialog is required therefore between registries for the completion of the transfer in both registries.

An external transfer deducts units from the balance of the transferor's account in order to add the same quantity to the balance of the transferee's account held in the receiving registry. The units transferred retain their unique serial number. Each registry automatically notifies the authorized users linked to the account it manages.

Different architectures link registries between them: one consists of linking each registry to all of the other registries (peer-to-peer as it is the case for the Verified Carbon Standard registry system) and the other consists of linking each registry to a central communication hub (as it is the case via the International Transaction Log for Kyoto Protocol national registries and via the European Union Transaction Log for EU ETS registries).

Only the central hub approach will be referred to in this document.

2.5.1. Accounting for an external transfer with a central hub

When a central hub is in place, each registry communicates with the hub and no registries are in direct communication with another (registry). The table below represents the accounting model for an external transfer.

Table 13 - Accounting for external transfers

	Transferring registry		**Receiving registry**	
	Transferor account		Account of the transferee	
	Debit	**Credit**	**Debit**	**Credit**
Account balance before transfer		Quantity Q1 T / P / L / t		Quantity Q2 T / P / L / t
Accounting model of a transfer of "q" units of type "T"	Quantity: **q** T / P / L / t Serial numbers: from x to y			Quantity: **q** T / P / L / t Serial numbers: from x to y
Account balance after transfer		Quantity: Q1-**q** T / P / L / t		Quantity: Q2+**q** T / P / L / t

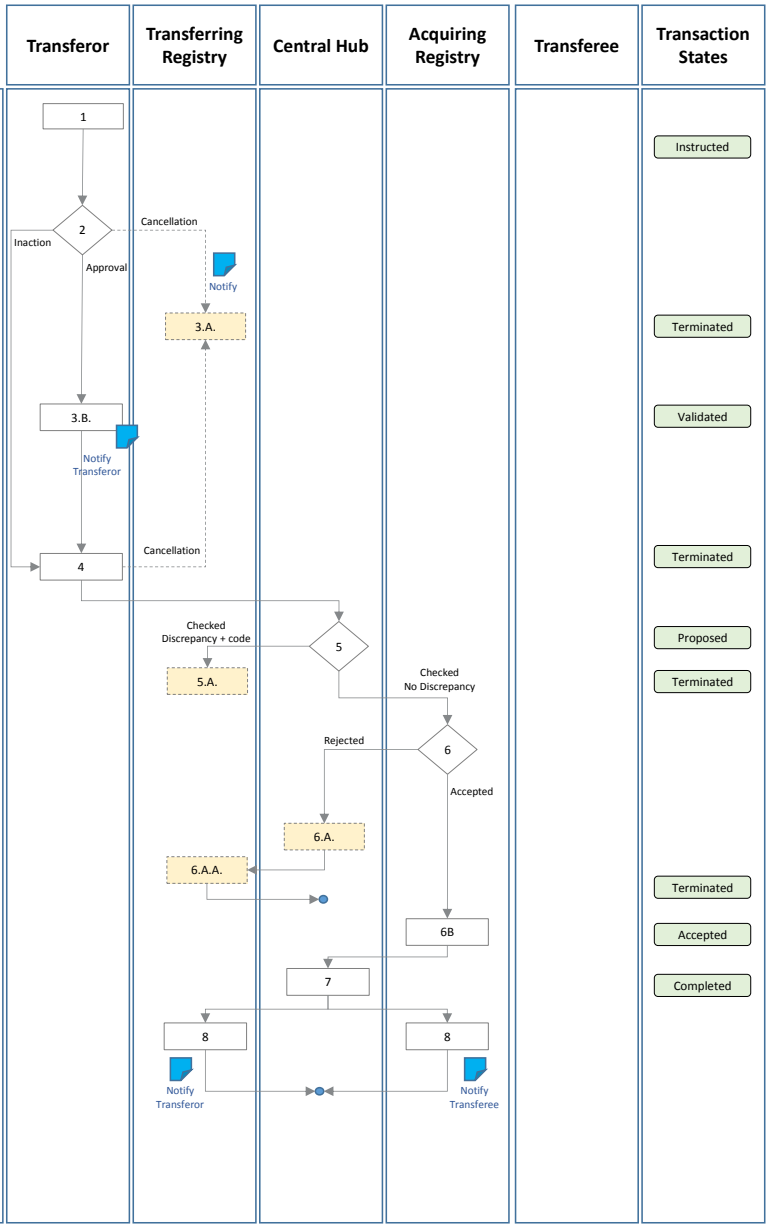
T / P / L / t = characteristics of the unit, T (type), P (Project), L (Label), t (validity period or vintage)

Once the transfer is completed, the units associated with the serial numbers transferred are no longer held in the transferring registry but in the receiving registry.

Figure 14 – External transfer: proposed workflow diagram

1. An authorized representative instructs the transfer to debit the transferor's account. The date of the transaction is automatically set to the current date.
2. Four-eye principle (optional): the transfer is reviewed by an authorized representative different from the one who authorized the transfer.
3. A. - The transfer is cancelled.
3. B. - The transfer is approved. (Based on optional security measures, such approval may require entering a password or an SMS code). The serial numbers affected by this transaction are no longer available for any transaction.
4. Option: after a certain time, an automatic decision may cancel or confirm the transfer.
Once approved, the transfer is notified to the central platform which carries out its own first level checks.
5.A. The central hub rejects the transfer.
6. The central platform proposes the transfer to the receiving registry. The receiving registry carries out its own checks (option: with explicit request for approval by the transferee)
6.A. The destination registry notifies the central hub of rejection of the transfer proposal which notifies the payer (6.A.A) who confirms receipt.
6.B. The destination registry accepts the proposal for transfer and notifies the platform.

7. The central platform notifies both registries.
8. Both registries post the transfer and produce notifications of successful transfer. The authorized representatives of the payer account and transferee account are notified by their respective registries. The central platform is notified of the successful completion of the transaction by each registry.

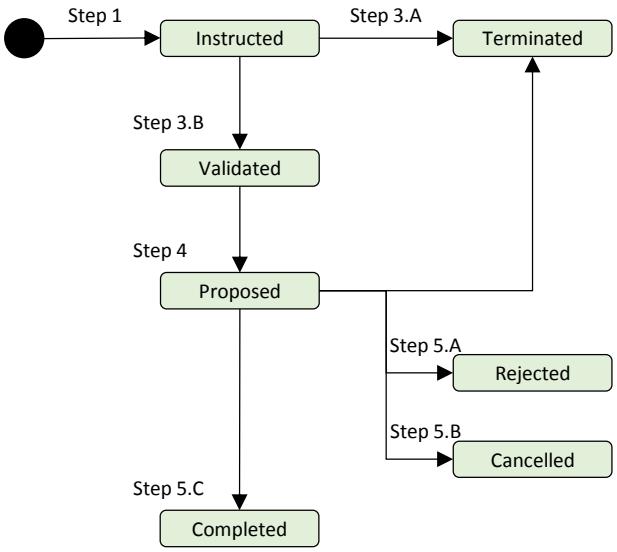


2.5.2. Statuses and change in status for an external transfer

The registry keeps an audit trail of statuses and status changes of all transactions.

The diagram below shows the status changes for an external transfer according to the workflow proposed above.

Figure 15 - External transfer – transaction status and status changes



2.5.3. Options and variants

- **Security measures and responsibilities of the transferor**

Before debiting the transferor's account, various security measures can be envisaged in order to limit the risk of operational error or fraud.

These measures can vary from a simple "out of band" notification (sending an SMS) to an explicit confirmation (re-entering password, validation by an authorized representative separate from the initiator of the internal transfer (4-eyes) or entering of a confirmation code received by SMS or a security token by one of the authorized representatives).

Other options can be envisaged before the transfer is proposed to the receiving registry:

- Automatic cancellation of any internal transfer entered and not validated before a certain configurable time lapse;
- Retraction period offered to authorize representatives of the transferor between the validation of the transfer and its presentation to the receiving registry.

- **Measures to ensure accountability of the beneficiary**

The registry can automatically notify the transferee of any transfer credited to one of his accounts. These notifications can be effected by e-mail or "out of band" via SMS for increased security.

An explicit validation by the transferee can also be requested for any transfer.

After a certain time lapse, a transfer received and not explicitly validated by the **transferee** can be automatically validated or rejected according to the design chosen by the designers of the receiving registry.

These measures are not only designed to reinforce the security of the system. These measures involve the explicit responsibility of the transferor and the **transferee** in the accounting for transfers and will protect "good faith buyers" against the risk of being required to return transferred units.

2.6. Cancellation

Cancellation in the wider sense represents the last stage in the life-cycle of a unit. The triggering event may be a manual instruction to cancel (or delete, withdraw, retire, surrender, restitute…) units initiated by an authorized representative to comply with the regulation (surrender units against verified emissions) or for voluntary offset, or a request from an authority (for example, subsequent to the detection of over-issuance). The triggering event may also be a planned event, such as the automatic cancellation of temporary or out-of-date units.

2.6.1. Accounting for unit cancellation

The cancellation will involve only one account holder: the transferor, owner of the units to cancel. The registry allows the user to choose the units to cancel, selecting notably the type of unit, the project, the label and the period.

The registry debits a quantity of units from the transferor's account unless the status of the account prohibits it (for example: account blocked or closed) and credits these units to the cancellation account, specific to various types of cancellation.

Opening different types of cancellation account allows for clearer accounting of different cancellation motives (voluntary cancellation, cancellation in accordance with regulation, cancellation following operational errors ...).

Once completed, a cancellation is definitive and irreversible: cancelled units and their serial numbers can no longer change accounts. Cancelled units retain their unique serial number. The registry automatically notifies authorized users linked to the transferor's account. The table below represents the accounting model for a cancellation.

Table 14 – Accounting model for a cancellation

	Transferor account		Cancellation account	
	Debit	**Credit**	**Debit**	**Credit**
Account balance before transfer		Quantity Q1 Type of unit: T		Quantity Q2 Caract*.: T / P / L / t
Accounting model for cancellation of "q" units of type "T"	Quantity: **q** Unit type: T Serial numbers: from x to y	→	→	Quantity: **q** Unit type: T Serial numbers: from x to y
Account balance after transfer		Quantity: Q1-**q** Unit type: T		Quantity: Q2+**q** T / P / L / t

T / P / L / t = characteristics of the unit, T (type), P (Project), L (Label), t (validity period or vintage)

The diagram below proposes a workflow for a cancellation with the addition of optional security measures. These options and their variants are then discussed.

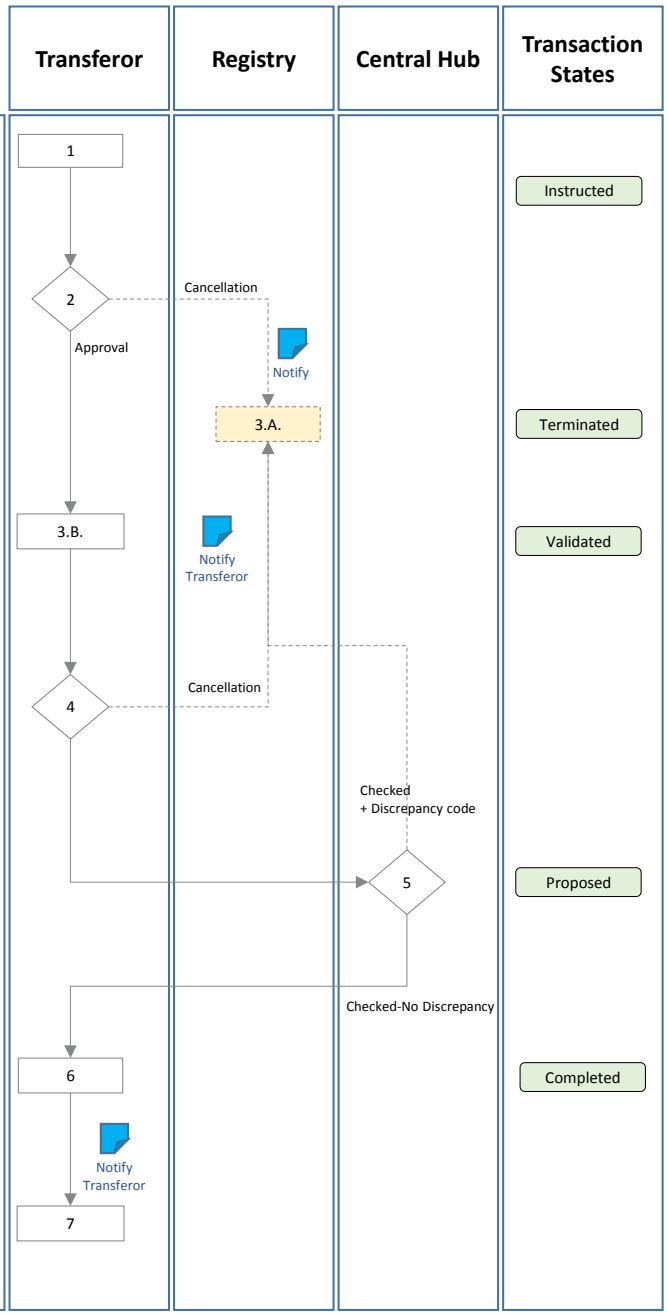
Figure 16 - Cancellation: Proposed workflow diagram

1. An authorized representative authorizes the cancellation of the withdrawal from the payer account. The date of the transaction is automatically set to the current date.
2. Four-eye principle (optional): the transfer is reviewed by an authorized representative different from the one who authorized the transfer.
3. A. – The transaction is cancelled.
3. B. – The transaction is approved. (Based on optional security measures, such approval may require entering a password or an SMS code). The serial numbers affected by this transaction are no longer available for any transaction.
4. Option: after a certain time limit without approval or explicit cancellation, the transaction can be automatically cancelled or non approval automatically recorded.

5. Option: the cancellation may be under the control of the central platform which may block or finalize it.

6. Once posted, the debited and credited account journals are updated.

7. The registry produces notifications of issuance which can be downloaded on-line. The authorized representatives of the payer account are notified.

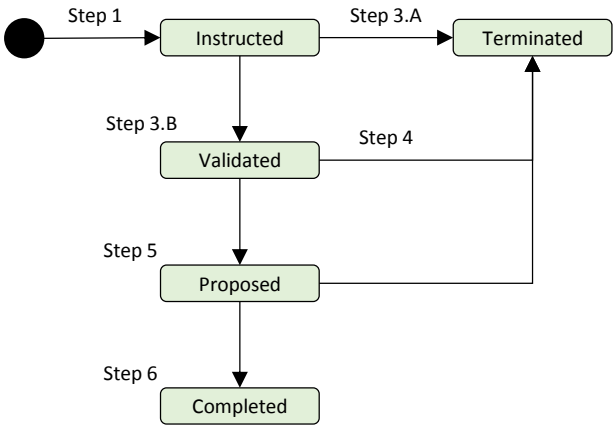


2.6.2. Statuses and change of statuses for a cancellation

The registry keeps an audit trail of statuses and status changes of all transactions.

The diagram below shows the status changes for a cancellation according to the workflow proposed above.

Figure 17 - Cancellation – transaction status and status changes



2.6.3. Options and variants

- **Security measures and responsibilities of the transferor**

Before debiting the transferor account, various security measures can be envisaged in order to limit the risk of inappropriate cancellation.

These measures can vary from a simple notification by e-mail or "out of band" (sending an SMS) to an explicit confirmation (re-entering password, validation by an authorized representative (distinct from the initiator of the cancellation (4-eyes)) or entering a confirmation code received by SMS or a security token by one of the authorized representatives).

Other security option: automatic cancellation of any cancellation transaction entered and non-validated after a certain configurable time lapse.

3. Administrative events

The registry offers several non-accounting functions to manage administrative events. These functions are available only to the team in charge of registry administration.

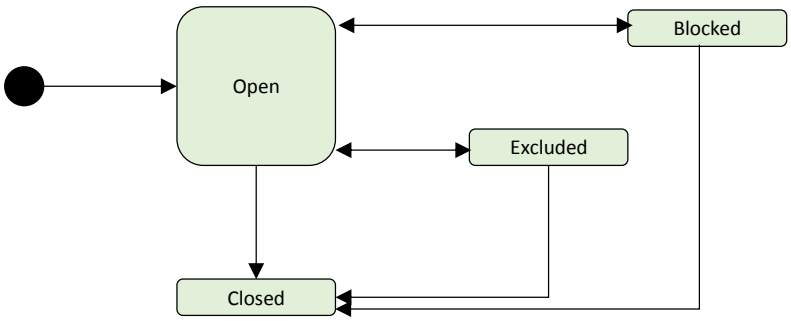
3.1. Managing accounts

The registry administrator can open (or refuse to open) an account, modify the status of an account, authorize or revoke user account authorization and close an account. Closure is permanent (no account in the future may be open using the same account identifier as a formerly closed account).

An account may have the following status: open, blocked and closed. In the case of ETS, the status "excluded" can be envisaged which embodies an account initially but no longer under regulatory compliance obligations (for example if the installation drops below the ETS eligibility limit).

A blocked account can no longer carry out operations, except depending on regulation in force, to comply with regulatory obligation.

Figure 18 – Account statuses and change of statuses



3.1. User management

Registry users are natural persons who represent the account holder and are authorized to carry out transactions on the account. These "authorized representatives" have authorization profiles which give them more extensive or fewer rights on a given account:

- Read only;
- Consultation and entering transactions; or
- Consultation, entering and validating transactions.

The registry administrator, subsequent to document control (“know your customer checks”), may attribute an authorization profile to a user.

Note: certain users may be mandated to manage the accounts of several account holders and may have different privileges for each account. The registry will therefore manages multiple authorizations for a single authenticated user, depending on the account this user is associated to.

Within the scope of the periodical review of users documentation, the registry administrator will update information relative to authorized representatives including their profile and the list of accounts to which they are attached.

3.2. Management of verified emissions

In the case of an ETS the registry administrator receives and enters (or imports by file) the verified emissions of each obliged installation.

The registry is therefore able to compare the verified emissions of an installation with the quotas surrendered by each installation and thus:

- Produce a conformity report for each installation ("compliance figures");
- Produce a report of compliant and non-compliant installations with, for the latter, the compliance shortfall; and
- Alert the relevant authorized representatives of the installation's account during surrender transaction entry, of any compliance shortfall or too excess in surrendered units.

3.3. Management of allocation tables

In the case of an ETS, the registry administrator can enter or import a file listing the amount of quota to be allocated to each installation (to be credited on each installation's account).

The registry offers a function which enables entry or import of this "allocation table".

The registry may also, on instruction from the regulator, execute an allocation process which consists of a set of internal transfers debiting the issuance account and crediting installations' accounts.

4. Traceability: audit logs, notifications and messages

The registry must retain, with no time limit[15], all transactions and administrative events which occur, with all their characteristics at each stage of the workflow: who entered them, when, with what values, who validated them, when and with what values, what notifications were sent to whom, by what means (including to what mobile telephone number (SMS) or e-mail address).

Certain particularly sensitive data require the archival of value change history, the date of each value change, the identity of each user who made a change and the previous value. This is the case notably for:

- Verified emissions of an installation and more generally, the level of obligation of an installation or a liable party (case of an ETS);
- Account status and account balances;
- The status of transactions;
- The type of account, even if the latter is not intended to be changed;
- The link between user and authorization profile; and
- The link between accounts and user, between accounts and account holder.

More generally, the registry updates logs which record all processes executed and all data changes.

[15] Unless specified otherwise by regulations in force

5. Main Business rules and alerts

5.1. Main business rules

R1. An account which holds serial numbers may never have a negative balance;
   a. The technical account debited on issuance does not hold serial numbers. Its balance is structurally "debit";
R2. An **account** number (identifier) is unique and never changes. An account in "closed" status retains its account number;
R3. A closed account cannot be reopened;
R4. A **transaction** number (identifier) is unique and never changes;
R5. A **user** number (identifier) is unique and never changes;
R6. An **account holder** number (identifier) is unique and never changes;
R7. An account type may not be changed. The definitive account type is associated with an account on opening;
R8. A unit cannot change serial number;
R9. At any given time a unit may be credited only to one account;
R10. A transaction must simultaneously debit one account and credit another;
R11. Registry transactions are carried out in real time. The definition of "real-time" is that of the Data Exchange Standard where applicable, and requires a precise definition in non-DES compliant registries;
R12. The registry enables the creation of new types of transaction with subsequent impact on accounting models (accounts which can or cannot be debited or credited);
R13. A transaction crediting a cancellation, deletion, retirement, restitution or surrender account (any account flagging the end-of-life of a unit) cannot be reversed;
R14. No transaction may debit a cancellation or deletion account;
R15. A surrender account can only be debited in order to credit another surrender account (for example: transfer from a surrender account for "liable parties" (e.g. obliged installations) to a State-level surrender account);
R16. The registry must comply with legal regulations in force;
R17. With the exception of the registry administrator, a user cannot enter a pre-dated transaction;
R18. With the exception of the registry administrator, a user cannot modify the date of a transaction;
R19. Any transaction can be annotated by the user who entered it or participates in its workflow, prior to the transaction’s completion (but not after). A text box is available for this purpose;
R20. The registry applies user authorization before any consultation, edit or modification is made possible;
R21. The registry does not allow the use of out of date units, nor does it allow for the use of credits issued by ineligible projects;
R22. An ETS registry may limit the maximum number of credits authorized for the conformity of each installation;
R23. The registry enables parameterization of restrictions on the use of certain types of units:

a. For certain types of transaction;
b. On certain types of accounts;
c. Depending on criteria related to projects (e.g.; host country, sectoral scope, registration year…).

5.2. Configurable alerts

Alerts are brought to the attention of the registry administrator or of registry users. Below are a few examples of events which generate alerts:

- Regulatory transactions expected but not yet completed;
- Accounts with a debit balance (other than the technical issuance account "-Q"). This situation should never occur and if it does, represents a technical system error;
- Pending transactions: transactions for which the last status in the workflow was not attained within “x” days of being entered or imported into the registry (configurable time lapse) or for units which will expire in less than “y” working days (configurable time lapse);
- Number of administrative operations on hold for more than “x” days (configurable time lapse);
- Transactions for which the accounting date differs from the date entered (later or prior);
- Discrepancies in compliance figures;
- Anomalies: differences (total amount and/or sign) between:
  - The sum of all account balances and the sum of all issued quantities;
  - The sum of all credits and the sum of all debits;

6. Main reports produced by the registry

The registry produces a set of reports to users, and provides the registry administrator with a catalogue of ad-hoc predefined and/or configurable queries.

6.1. Reports to account holders (non-modifiable)

The following reports are made available:

- Transaction notification : this report is made available to users authorized on both accounts affected by the transaction;
- Account balance at date : shows the balance of an account, split by unit type;
- History of end of month account balances between two dates : shows a table listing balances split by unit type, on a given account;
- History of transactions between two dates : shows a table listing all transactions completed on a given account;
- Transaction status change history: shows a table listing all status change for a given transaction.

6.2. Library of predefined queries

The registry administrator may query the database using queries.

These queries are developed in such a way that the registry administrator does not require the intervention of IT personnel. Queries will be run on a copy of the database, so that the registry IT performances will not be altered.

To this end, the registry offers a library of queries. Each query has associated a title, delivery dates and a comment which describes the result.

The result of the query is generally a downloadable file in CSV format. The list below shows a list of common requirements for such queries:

- **List of users** and all their attributes: identifier, title, name, first name, address, login, mobile telephone number, e-mail, fax number, identify and title of authorization profile, identifier and business name of employer...
- **List of accounts** and all their attributes: identifier, designation, type of account, status of accounts, identifier and business name of account holder, identifier and business name of lead manager, identifier and business name of the authorized representative, identifier, name and first name of each user, user rights on the account (RAA, RA, Auditor) account balance at query date for each delivery year…
- **List of account holders** and all their attributes: identifier, identifier of contract with registry administrator, contract date of effect, contract end date, login, account holder business name…
- **List of blocks of serial numbers held** year of issuance, site, credit account on which the blocks are held at the query date, label, vintage or year of issuance, type of unit…

- **List of transactions** with all attributes notably those present on the transaction receipt…
- **Configurations tables**: table of correspondence between functions and profiles; list of accounting schemes by type of operation...

7. Registry website

The registry and its website may manage several display languages. The registry website may also supplement the registry with other functions as illustrated hereafter.

7.1. Management of passwords

The management of forgotten or renewed passwords must incur to the users and therefore will incur a minimum workload for the registry administrator / operator. The registry offers an autonomous secure process to all users to manage their password.

Other requests from the user require validation by the registry administration before taking effect, notably changes related to name, telephone number (important when used for SMS notifications) address, authorization profile or access rights to an account.

7.2. Information banner

The banner displayed on the public home page is available to all. A specific banner is displayed on the welcome page for duly authenticated users.

The public welcome page banner is managed independently of the specific banner for authenticated users.

The administrator has access to a service which enables him to update the contents of the information banner.

7.3. Applicable regulations

List of links to official regulations which cover the Market Mechanism.

7.4. Documents for download

This page offers a set of documents for download:

- Contracts and agreements (public);
- General on-line usage conditions (public);
- Prices (public);
- Account opening procedure (public);
- Registry user guide (available only to connected users).

7.5. FAQ

Available only to connected users and regularly updated by the registry hotline.

7.6. Legal notices

As necessary, legal notices on limited responsibility and personal data management.

D- TECHNICAL SPECIFICATIONS

1. Introduction

By "Contract Holder" it is understood the supplier appointed to provide registry services.

By “Competent Authority” it is understood the entity contracting with the “Contract Holder” (e.g. the regulator or the registry administrator).

This chapter is written in the form of a technical guide to follow step-by-step to specify security and other technical information system requirements. However, it is assumed that each “Competent Authority” will adapt or remove the following proposals to fit to their requirements and specific situation.

All security measures applied to production data also apply to archived data.

2. Technical requirements

2.1. Location of registry data hosting

Detail whether who has responsibility for service and data hosting, the reservation of the domain name (the Contract Holder, the Competent Authority, or another entity).

Detail the case being, restrictions concerning the location of data centers and the conditions required to change data center during the life of the contract.

2.2. User access to the registry via internet

The registry must be accessible securely to all users by Internet.

In order to make sure that access to the registry is protected and reserved to authorized users, specific requirements may be envisaged. E.g. require secure https protocol on port 443 (with robust encryption algorithms: SSLv3 / TLSv1 obligatory) and obligatory strong authentication for all users.

Further user access security strengthening measure can be envisaged such as imposing that access to the registry by users from their workstations is only possible via a standard Internet navigator (i.e. "thin client"). In that case, clarifying which versions of the main internet navigators must be completely supported by the registry may prove useful to limit the scope of maintenance and testing.

In order to ensure compatibility of the registry provided by the contract holder, it is recommended to describe the computing environment for access to the registry by the registry administrator. Especially, details can be provided regarding:

- Type of workstation and operating system, navigator(s) used and notification period required by the Contract Holder before any change is made to this environment;
- Mode of access to Internet (network and security equipment, obligatory servers (proxies));

- Requirements for functional tests of user technologies in the registry environment.

Depending on the Competent Authority specific requirements, certain technologies are to be banned. It is recommended to explicitly list them. For example, registries requiring or using following technologies may not be accepted:

- Installation of software on the workstation;
- That the user has specific rights on his workstation (e.g. administrator rights);
- Runtime execution environment such as Java (JRE - Java Runtime Environment), applets, ActiveX, "plug-ins" (Flash / Flex ...) with the exception of plug-ins for formatting and printing documents (such as Acrobat Reader).

Lastly, it can be specified if access from mobile devices is required.

2.3. Documentation

It is recommended to impose some obligations of the Contract Holder with regard to the frequency of documentation update to the competent authority, notably: **architecture documentation** and **production documentation,**) which cover all hosting solutions.

The **architecture documentation** describes notably, the computing hardware, software and versions, data flows and volumes, implemented redundancy, environment and hosting infrastructure and services which achieve the levels of service expected. The architecture documentation also describes the mechanisms implemented in order to guarantee AICT service levels (availability, integrity, confidentiality, traceability) and all security requirements as well as compliance to an industry security standard (example: ISO 2700x).

The **production documentation** describes backup plans, data purging and archiving, monitoring and internal escalation of incidents and escalation procedures to the competent authority in case of crisis.

2.4. Environment and production implementation process

It is recommended to detail requirement regarding access to computing environments by the competent authority or the registry administrator: training environment, test environment, pre-production environment, and production environment.

It is recommended to stipulate that delivery of new functionality must pass through the test environment and requires sign off from the application owner to move into production.

It is recommended to stipulate if “volume tests” (i.e. benchmark) are required with real-life data or not. Where real-life data is required, it is recommended to clarify if those data must be encrypted or not.

It is recommended to specify if a distinct backup site is required and if so, to clarify if following requirements are to be fulfilled:

- Synchronization of data in real-time and the guarantee that no information will be lost in case of failure of the main hosted site;

- A test of the registry backup before commissioning the registry with a test report submitted to the competent authority;

2.5. Registry launch phase

It is recommended to detail the test phases required for commissioning the registry and the time-scale required to correct defects detected against the general functional specifications.

It is recommended to detail the guarantee period after commissioning (launching) of the registry during which defects will be corrected without charging any additional cost.

2.6. Registry availability

In order to clarify when the registry must be available, it is recommended to consider clarifying:

- The working hours during which the registry will be available to users and as necessary, distinguish access by the registry administrator from other users. Determine if delivery of functionality will occur during or outside of these working hours.
- The notification period for any requests for availability outside of these working hours.
- The conditions that the registry must adhere to be considered effectively available.
- The effective availability rate required for the registry detailing the formula used to calculate this service level indicator.
- The Maximum tolerable period of disruption (MTPOD) during working hours in number of consecutive hours.

The reliability of the registry requires, that the Recovery Point Objective (Maximum Acceptable Data Loss rate) is equal to zero.

2.7. Data archiving

It is recommended to detail the rules for accessing on-line archive data by the registry administrator.

2.8. Performance

It is recommended to provide detailed requirements in terms of processing time, (execution of processes such as authentication, posting a transaction or opening an account).

It is also recommended to detail requirements for performance monitoring: reporting frequency, incident report contents, their causes and steps taken to repair them, independent audits etc.

It is recommended to define performance indicators such as:

- Measured availability rate of registry functions;
- CPU usage rate;
- The number of inputs / outputs;
- Bandwidth used;

- Memory capacity used;
- Volumes and frequency of transactions, in a day and over the course of the year;
- Measure of average, min. and max. Response time over the period of the report.

2.9. Data exchange between the registry and other information systems

It is recommended to establish the list of other information systems with which the registry exchanges data and specify the format and communication protocol of these exchanges.

It is recommended to require the implementation of a file server if the registry exchanges files via Internet,

It is recommended to provide detailed requirements in terms of data encryption exchanges, for example the use of SFTP secure protocol (SSH File Transfer Protocol) and encryption and authentication for interconnected systems.

It is recommended to require that Data exchange folders must adhere to the same security and confidentiality requirements applicable to the registry.

It is recommended to require that the list of files exchanged with the registry must be included in monitoring reports produced by the Contract Holder.

3. Security requirements

This chapter especially details recommendations regarding security requirement in terms of integrity and confidentiality, availability, traceability of data, authentication, management of incidents and security audits.

3.1. Session expiry

It is recommended to detail the duration of inactivity after which a user session will time-out.

3.2. Integrity and confidentiality of data

It is recommended to require that the Contract Holder should detail the computing and organizational facilities implemented to guarantee integrity and confidentiality of data, protection against disclosure, and unauthorized modification of data, notably between users and between applications hosted on the same server.

It is also recommended to require that the Contract Holder shall not use client or user data for any other purpose other than those stipulated in the Contract. In particular they must not be transmitted to a third party and under no circumstances be used for commercial ends.

3.3. Availability

It is recommended to ask the Contract Holder to detail measures protecting against all types of service denial attack.

3.4. Traceability

Over and above data traceability requirements described above in this document (see paragraph “C- Functional specifications” sub-paragraph dedicated to traceability), it is recommended to require that the contract holder shall ensure the traceability of all technical events such as (non-exhaustive list):

- The connection and disconnection of technical accounts (i.e. system accounts, application accounts, administrative accounts, etc.);
- Actions carried out through technical accounts;
- All individual access to databases;
- Password changes on technical accounts;
- Creation, deletion and modification of access rights to technical accounts.

It is also recommended to detail the length of time that these elements will be held on archive by the contract holder.

3.5. Authentication

It is recommended to require at least two authentication factors: one related to something that the user knows (password, secret question ...) and one related to something that the user possesses (ex: SMS, token PKI certificate).

It is recommended to require a password update service. This service should allow the user to request the re-initialization of his personal password and to receive an email by return. The e-mail contains an unblocking code (or One Time Password) which allows the user to choose a new password on next connection.

It is also recommended to require that a password policy is in place, imposing especially that the password is not an easily guessed one and should be changed frequently.

3.6. Management of security incidents

It is recommended to require that the contract holder implements a security system including incident management procedures and including:

- Detection of security alerts;
- Keeping tracks the incident until it's effective closure;
- Implementing the recommendations made following a security incident;
- Informing immediately and coordinating with the Competent Authority in the event of any major incident;
- Supplying a monthly dashboard monitoring security incidents to the Competent Authority.

It is recommended to require that management of security incidents shall also include the management of platform vulnerabilities and the management of security patches made available by editors.

3.7. Security audits

It is recommended to require that the contract holder describes the information system Security strategy notably the choice of standards to adhere to, performance monitoring indicators, system availability, quality of service, security architecture (firewalls, DMZ, application and data layer reporting, VPN, WAN / LAN, redundancy for critical services etc.).

It is recommended to impose that the Contract Holder authorizes the competent authority to proceed with, or contact a third party to carry out regular audits of the registry in order to:

- Ensure that practices adhere to the directives of the contract and requirements of the general functional specifications;
- Ensure that the registry is not vulnerable to events which could impact the availability, integrity, confidentiality and traceability of data;
- Ensure that recommendations from previous audits have been correctly implemented.

Audits may be configuration audits, intrusion tests, organizational audits, physical audits on the service provider's site.

It is highly recommended to require an audit to be carried out before the commissioning of the registry to implement monitoring and control processes.

E- COMMON RECOMMENDATIONS AND GUIDANCE ON THE DEVELOPMENT OF THE REGISTRY TECHNICAL INFRASTRUCTURE

(a)	A Request For Interest (RFI) may help to improve knowledge of existing offers and potential providers
(b)	Assess volumes, risks and required level of security
(c)	Make decisions on: - The scope and nature of the service sought - Procurement options (i.e. development from scratch, adaptation of existing software or SaaS) - Registry connectivity options
(d)	Draft Functional Specifications: - List applicable business rules - Inventory data related to users, accounts and units - List the accounts types and transactions types needed - Describe the workflow related to each transaction type - List any other functions required and define authorizations profiles access to these functions - Provide templates for all reports and notifications - Describe the web pages of the registry's website
(e)	Drafting the Technical Specifications: - Technical architecture including hosting, archiving and performances - Security requirements including authentication, confidentiality, traceability and security audits.

Annex 1. Indicative list of functions to develop and profiles which have access

A: System administrator profile
B: Registry administrator profile
C: Registry operator profile
D: Authorized representative profile
E: Additional authorized representative profile
F: Account auditor profile
G: Unique representative profile
H: MRV report verifier profile

Table 15: List of registry functions

Type of process	Process	Specific process (as necessary)	A	B	C	D	E	F	G	H
Administration	Registry Administration dashboard		☑	☑	☑					
Administration	Configure the system	Functional	☑	☑						
Administration	Configure the system	Technical	☑							
Administration	Manage an alert (function provided to the registry administrator)	The whole registry	☑	☑	☑					
Administration	Manage an alert (function provided to the users)		☑	☑	☑	☑	☑		☑	
Administration	Open an account			☑	☑					
Administration	Modify the status of account			☑	☑					
Administration	Create a new authentication profile			☑	☑					
Administration	Change an authentication profile			☑	☑					
Administration	Consult an authentication profile		☑	☑	☑					
Administration	Export authentication profiles		☑	☑	☑					
Users	Change a password		☑	☑	☑	☑	☑	☑	☑	

Type of process	Process	Specific process (as necessary)	A	B	C	D	E	F	G	H
Administration	Revoke a password		☑	☑	☑					
Account	Modify an account		☑	☑	☑					
Account	Consult the list of accounts (for which the user is authorized)		☑	☑	☑	☑	☑	☑	☑	
Account	Consult the detail of account		☑	☑	☑	☑	☑	☑	☑	
Account	Consult the history of account balances		☑	☑	☑	☑	☑	☑	☑	
Administration	Create a user		☑	☑	☑					
Administration	Modify a user		☑	☑	☑					
Administration	Authorize a user		☑	☑	☑					
Administration	Modify user authorization		☑	☑	☑					
Administration	Authorize an administrator or registry operator		☑	☑						
Administration	Modify the authorization of an administrator or registry operator			☑	☑					
Account	Authorize an account user			☑	☑					
Users	Revoke a user		☑	☑	☑					
Transactions	Enter an operation	Issuance		☑	☑					
Transactions	Enter an operation	Allocation		☑	☑					
Transactions	Enter an operation	Cancellation		☑	☑					
Transactions	Enter an operation	Internal transfer		☑	☑	☑	☑		☑	
Transactions	Enter an operation	External transfer		☑	☑	☑	☑		☑	
Transactions	Enter an operation	Unit surrendering (ETS)		☑	☑	☑	☑		☑	
Transactions	Enter the verified emissions of an installation			☑	☑					☑
Transactions	Import a file of verified emissions		☑	☑	☑					
Transactions	Import an “allocation table”		☑	☑	☑					
Transactions	Validate verified emissions			☑						☑

Type of process	Process	Specific process (as necessary)	A	B	C	D	E	F	G	H
Transactions	Validate a transaction			☑	☑		☑		☑	
Transactions	Cancel a validated transaction			☑	☑	☑	☑		☑	
Transactions	Cancel a transaction			☑	☑	☑	☑		☑	
Transactions	Approved a transaction			☑	☑		☑		☑	
Transactions	Refuse a transaction			☑	☑		☑		☑	
Transactions	Consult the list of transactions awaiting further action		☑	☑	☑	☑	☑	☑	☑	
Transactions	Consult the list of posted transactions		☑	☑	☑	☑	☑	☑	☑	
Transactions	Consult the detail of a transaction		☑	☑	☑	☑	☑	☑	☑	
Administration	Consult alerts and notifications		☑	☑	☑	☑	☑	☑	☑	
Administration	Cancel an alert / notification			☑						
Transactions	Consult the history of operations between two dates		☑	☑	☑	☑	☑	☑	☑	
Administration	Emergency stop: registry unavailable for customers		☑	☑	☑					
Administration	Emergency stop: registry unavailable for all users and the public		☑	☑						
Administration	System restart		☑	☑						
Transactions	Consult / Download a transaction receipt / account balance		☑	☑	☑	☑	☑	☑	☑	
Administration	Enter information to publish on the public registry welcome page		☑	☑	☑					
Administration	Enter information to publish on the welcome page for authenticated users		☑	☑	☑					
Administration	Export the list of Natural Persons and companies (name, first name, title, company name, address, e-mail, landline / mobile / fax number, formatted postal address, etc.		☑	☑	☑					
Administration	Upload documents to make available on the public website		☑	☑	☑					

Annex 2. Potential requirements to update DES reference nomenclatures based on registry developments

Whether connecting to the ITL in the future or not, Market Mechanisms may choose to use the DES which is an existing standardized communication protocol to exchange information between registries.

Procedures could be implemented which would enable Market Mechanisms to reserve reference values for codes and nomenclatures laid out by the DES (even to create new reference nomenclatures, for example for labels). Several examples below:

Where in the DES	Code	Reserved values	Example of new values which may be required
Annex G Fig. 1	Type of account	100 ...423	Risk buffer account Project proponent account Surrendering account (by liable parties) Nostro account Vostro account
Annex G Fig. 4	UTCF/LULUCF activity	1 to 7	Types used by REDD+, by voluntary standards and by Market Mechanisms
Annex G Fig. 5	Notification status	1 to 3	No requirements identified
Annex G Fig. 6	Type of notification	1 to 11	Question not asked
Annex G Fig. 7	Participant status	1 ; 2	Source registry (for the case of a transfer between Nostro / Vostro non-emitting (accounting) registries)
Annex G Fig. 8	Reconciliation status	0 to 11 ; 98 ; 99	Question not asked
Annex G Fig. 9	Transaction status	1 to 16	Question not asked
Annex G Fig.10	Transaction type	1 to 10	No requirement identified if the risk buffer account has its own type. Otherwise, requirement for a dedicated type of transaction for buffer provision and buffer release.
Annex G Fig.11	Type of unit:	1 to 7	Types of units of voluntary standards and of each new Market Mechanism

Annex 3. Analytic framework to compare registries

The following table summarizes the main characteristics of a registry in order to be able to compare.

Id.	Characteristic
	Administration
1.	Is the administration of the registry conferred on a public or private entity (or detail the company name and the type of entity)?
2.	Is the registry administrated by distinct levels of legal jurisdiction (national, provincial, regional ...)?
3.	How many users (Natural Persons) use the registry?
4.	How many accounts are open in the registry?
5.	How many (equivalent of) full-time staff administer the registry?
6.	How many liable party accounts (obligatory participation)?
7.	What are the working hours for which the registry is accessible on-line users?
8.	What are the main security measures implemented?
	Connectivity
9.	Is the registry connected to other systems (MRV, trading platform ...)? List them.
10.	Is the registry connected to other registries? How many?
11.	If the registry is connected to at least one other registry: how are external transfers accounted for (inventory entry / exit; Nostro / Vostro ("correspondent banking"); other (specify)…).
12.	If the registry is connected to at least one other registry: is the connectivity architecture based on peer-to-peer or based on a central hub?
13.	If the registry is connected to at least one other registry: is the communication protocol specific, or standard (which standard (Swift, DES …)? (Detail the main characteristics of this protocol).
14.	Does the registry manage types of transactions other than issuance-allocation-transfer-cancelling? If yes (example: buffer provisions / buffer release or surrendering), detail.
15.	Does the registry manage types of account other than obligatory holding (operators, liable parties, states, jurisdictions) - voluntary holding (brokers...) – technical (cancellation; auctions)? If yes which and why?
16.	What type of units are accounted for by the registry?
17.	What labels are managed by the registry?
18.	What authentication profiles are offered to registry users? (Example: data entry, entry and validation, read only).
19.	Was the registry IT developed from scratch, or adapted from existing solutions, or "rented" on use (SaaS)?
20.	What kind of external support has been sought in order to implement an operational registry:: - To synthetize business requirements and lay down functional specifications? - To lay down IT technical specifications? - To provide development, hosting and maintenance services? - To provide hotline services? - To provide all or part of the registry administration services (initial contact, follow-up / updating of documents relative to account holders ...)?