



**Standards and recommended practices for electronic
recording of data and information related to internationally
transferred mitigation outcomes**

Version 1.0

Contents

	<i>Page</i>
I. Introduction	4
A. Mandate	4
B. Applicability	4
C. Objectives	4
II. Guiding principles	5
III. Formats for identifiers and related elements	6
A. Party identifiers	6
B. Cooperative approach identifiers	6
C. Authorization identifiers	6
D. Registry identifiers	7
E. Account types	7
F. Account identifiers	8
G. Mitigation outcome (including authorized mitigation outcome and ITMO) unique identifiers	9
H. Transaction identifiers	9
I. Internet standard date-time stamps	10
IV. Attributes for primary entities	11
A. ITMOs and authorized mitigation outcomes	11
B. Transaction	12
C. Account	14
V. Recommended practices	16
A. Transaction and data integrity	16
Annex III – Definitions	18

Abbreviations and acronyms

AEF	Agreed electronic format
CARP	Centralized Accounting and Reporting Platform
CMA	Conference of the Parties serving as the meeting of the Parties to the Paris Agreement
ISO	International Organization for Standardization
ITMO	Internationally Transferred Mitigation Outcomes
MIME	Multipurpose Internet Mail Extensions
NDC	Nationally Determined Contribution
RFC	Request for Comments
RSA	Registry Systems Administrators
UML	Unified Modeling Language
UTC	Coordinated Universal Time

I. Introduction

A. Mandate

1. Decision 6/CMA.4, paragraph 32, requests the secretariat to develop, publish and periodically update, for participating Parties opting to apply the guidance referred to in annex I, chapter I.B, **standards and recommended practices for electronic recording of data and information related to internationally transferred mitigation outcomes**, and communication standards for interoperability and transactions with ITMOs, including record-keeping arrangements, data security protocols, risk management and disaster recovery procedures, and other practices, as necessary, including with inputs from the RSA forum.
2. This document contains the standards and recommended practices for electronic recording of data and information related to ITMOs (hereunder “these recommended practices”).

B. Applicability

3. These recommended practices are intended for use by participating Parties opting to apply the guidance referred to in annex I, chapter I.B of decision 6/CMA.4.
4. These recommended practices may also prove beneficial, in whole or in part, to all other participating Parties and to entities recording data and information related to ITMOs.

C. Objectives

5. The guidance in decision 6/CMA.4, annex I, chapter I.B describes two primary objectives for these recommended practices:
 - (a) **Mitigate data consistency risks:** “Implement appropriate standards and procedures to mitigate risks to the consistency of data, including through communication of data about the transfer and reconciliation procedures within and between registries”;
 - (b) **Ensure non-repudiation:** “Interoperability of registries should be implemented in such a way that neither Party to an inter-registry transfer could later repudiate the existence, type, time or content of the transfer”.

II. Guiding principles

6. These recommendations have been elaborated to achieve:
 - (a) Robust accounting: information concerning ITMO transactions are documented and recorded accurately, and ITMO holdings, when reported, reflect the true position of a registry;
 - (b) Avoidance of double counting: ITMOs are only located in one account at any given time and maintain strict consistency between balances of ITMOs in each account and their ledger. Real-time consistency checks are performed at the time of transaction proposal, frequent reconciliations are undertaken, and in the event of an inconsistency, a predictable process for resolving it is in place.
7. Using a single, standard format of identifiers across Parties enables robust accounting and avoidance of double counting.

Even for Parties that opt not to interoperate according to the Communications Standards, use of these standards will enable automated systems to effectively and efficiently track and trace ITMOs and transactions without the need for human intervention, in order to map and equate the same entity, identified by different names and identifiers, for example, across AEF submissions.
8. Where industry standards already address requirements, the industry standards should be used, as they are already documented, widely distributed and understood.
9. Each participating Party MUST submit, on an annual basis, information in an agreed electronic format (AEF) pursuant to annex, chapter IV.B of decision 2/CMA.3 through the submission portal of the CARP according to annex I, chapter II.A of decision 6/CMA.4. The submission portal SHALL have a human- and machine-readable interface for uploading information, including for recording data in the Article 6 database pursuant to decision 6/CMA.4, annex I, chapter II.A.
10. The secretariat has also published and maintains two related documents:
 - (a) Communication standards for interoperability, that adhere to these recommended practices;
 - (b) List of common nomenclatures under Article 6, paragraph 2, of the Paris Agreement, that, if inconsistent with these recommendations, take precedence.

III. Formats for identifiers and related elements

A. Party identifiers

11. Parties are identified using the ISO 3166-1 alpha-3 code of the corresponding country. The use of alpha-3 codes, rather than alpha-2 codes, provides clearer differentiation between countries whose names share similar prefixes.
12. As the European Union is a Party to the Paris Agreement, but not a country, it is assigned the user-assigned code element “XEU”. The prefix “X” indicates that the Party does not correspond to a country. Additionally, the code “XMR” is reserved for the Article 6.4 mechanism (registry).
13. For testing purposes, where it is necessary to define identifiers that do not correspond to a country, user-assigned code elements may be used from the range ZZA-ZZZ. Such test identifiers must not be used in a production environment.

Examples

DEU – Party identifier for Germany
XEU – Party identifier for the European Union
XMR – Identifier for the Article 6.4 mechanism (registry)
ZWE – Party identifier for Zimbabwe
ZZZ – A test registry

B. Cooperative approach identifiers

14. The format of a cooperative approach identifier is "CA<NNNNNN>" where "CA" is the fixed prefix and <NNNNNN> is a six-digit numeric sequence that is incremented by one for each additional cooperative approach.

The previously defined format of a cooperative approach identifier was "CA<NNNN>" with a four-digit numeric sequence. Accordingly:

- Cooperative approach identifiers using the four-digit format will continue to be recognised;
- Cooperative approach identifiers in the four-digit and six-digit formats that represent the same integer value are considered identical. For example, "CA0031" and "CA000031" refer to the same cooperative approach.

Examples

CA000001 – Article 6.4 mechanism (between Parties to the Paris Agreement)
CA000019 – Joint Crediting Mechanism between the Government of Japan and the Republic of Kenya

C. Authorization identifiers

15. Authorization identifiers conform to the pattern:

“AZ_<Party identifier>_<NNNN>”

where:

<NNNN> is a four-digit sequence number assigned incrementally, starting from 0001, and unique within the Party identifier.

Examples (hypothetical)

AZ_DEU_0001 – The first authorization for Germany
AZ_THA_0002 – The second authorization for Thailand

D. Registry identifiers

16. Registry identifiers consist of two components:

- (a) The Party identifier as described in section A above; and
- (b) A two-digit sequence number, unique within each Party identifier, assigned incrementally by the Party starting from 01.

The registry identifier is formed by concatenating these two components without any separator.

Examples (hypothetical)

KHM01 – The first registry of Cambodia
BRA01, BRA02 – The first and second registries of Brazil
XMR01 – The Article 6.4 mechanism registry

E. Account types

17. Account types enable robust accounting by ensuring that the source and destination accounts of ITMO transactions are consistent with the purpose of the transaction. The numerical value assigned to an account type identifies the purpose of the account. The list of account types is provided in Table 1.

Table 1 - Account types

<i>Value</i>	<i>Description</i>
100	Holding Authorised MOs are registered to 100 Holding accounts. ITMOs are transferred to and from 100 Holding accounts. See decision 2/CMA.3, annex, para. 29. Note: if a participating Party registry requires Pending and/or Authorized entity holding accounts, or additional types of holding accounts, it is its responsibility to determine how it will identify these account subtypes within its registry, as long as it transfers ITMOs to and from other registries using 100 Holding accounts. Pending, Holding, Party holding, Authorized entity holding, and Share of proceeds of adaptation accounts in the Art 6.4 mechanism registry are considered 100 Holding accounts (see decision 3/CMA.3, annex, paras. 58, 60 and 63).
200	Use towards NDC When an ITMO is used towards NDC, it is transferred from a 100 Holding account to a 200 Use towards NDC account located in the same registry. See decision 2/CMA.3, annex, para. 29.
210	Use towards international mitigation purposes (IMP) When an ITMO is used towards IMP, it is transferred from a 100 Holding account to a 210 Use towards international mitigation purposes (IMP) located in the same registry. See decision 2/CMA.3, annex, para. 29 and decision 4/CMA.6, annex, table 3, footnote u.

<i>Value</i>	<i>Description</i>
300	Cancellation for other purposes (OP) When an ITMO is cancelled for other purposes (OP), it is transferred from a 100 Holding account to a 300 Cancellation for other purposes (OP) account located in the same registry. See decision 2/CMA.3, annex, para. 29 and decision 4/CMA.6, annex, table 3, footnote u.
310	Voluntary cancellation of ITMOs not counted towards NDC or OIMP, for OMGE When ITMO not counted towards NDC or OIMP are voluntarily cancelled for OMGE, it is transferred from a 100 Holding account to a 310 Voluntary cancellation of ITMOs not counted towards NDC or OIMP, for OMGE, located in the same registry. See decision 2/CMA.3, annex, para. 39.
320	Voluntary cancellation When an ITMO is cancelled voluntarily for a purpose other than those specified in account type 300, 310 and 330, it is transferred from a 100 Holding account to a 320 Voluntary cancellation account located in the same registry. See decision 2/CMA.3, annex, para. 29 and decision 3/CMA.3, annex, para. 61.
330	Administrative cancellation When an ITMO is cancelled for administrative reasons, it is transferred from a 100 Holding account to a 330 Administrative cancellation account located in the same registry. See decision 2/CMA.3, annex, para. 29.

F. Account identifiers

18. Account identifiers conform to the IBAN standard.
19. The IBAN consists of up to 34 alphanumeric characters, as defined by the international standard under ISO 13616-1:2020. It is comprised of (in order):
 - A country code – 2 letters (ISO 3166-1 alpha-2 code)
 - The code EU is reserved for the European Union
 - The code XM is reserved for the Article 6.4 mechanism registry
 - Check digits, calculated using MOD-97-10 as per ISO/IEC 7064:2003 – 2 digits
 - BBAN – Between 11 and 30 alphanumeric characters
20. The BBAN structure is specific for each two-letters prefix (i.e. country code).
21. Each registry is responsible for generating account identifiers that conform to the IBAN standard and are unique within that registry. Once assigned, an account identifier must not be reassigned to another account.
22. When registries process transactions involving account identifiers, they should verify the validity of these identifiers by verifying the check digits.

Examples (hypothetical)

GB29NWBK60161331926819 – is a UK IBAN

NO8330001234567 – is Norwegian IBAN

RU0204452560040702810412345678901 – is a Russian IBAN

G. Mitigation outcome (including authorized mitigation outcome and ITMO) unique identifiers

23. For the purposes of brevity, this section, the term "mitigation outcome" refers to units of (yet to be authorized) mitigation outcomes, authorised migration outcomes, and ITMOs, where applicable.
24. Mitigation outcomes are referenced and transacted in blocks of units rather than individual units. Consequently, identifiers are assigned to blocks of units.

The identifier for a block of mitigation outcomes is composed of two parts:

(a) Originating Party registry identifier

The originating Party registry identifier is the identifier of the registry of the Party that authorised the underlying mitigation outcome.

The originating Party registry identifier is included in the unique identifier of mitigation outcomes because the originating Party registry is responsible for generating the unique identifiers. This enables the originating Party registry to manage serial number ranges and ensure that all mitigation outcomes it creates have distinct identifiers and do not overlap.

(b) First serial number and last serial number¹ – serial number range

Each block of mitigation outcomes has a first serial number and a last serial number, which inclusively define the start and end sequence numbers of the block.

Within each originating Party registry, serial number ranges do not overlap.

25. When stored or communicated electronically, the unique identifier for blocks of units consists of three elements:
- originating Party registry identifier;
 - first serial number; and
 - last serial number.
26. When represented as a textual string, the three elements are separated by a space-padded hyphen (" - "), and serial numbers use a space (" ") as the thousands separator.

Examples

CHE01 - 2 045 632 - 3 141 592	the block of 1 095 961 mitigation outcomes registered by the registry CHE01 with a first serial number of 2 045 632, and a last serial number of 3 141 592
THA01 - 1 024 - 434 963	the block of 433 940 mitigation outcomes registered by the registry THA01, with a first serial number of 1 024, and a last serial number of 434 963

H. Transaction identifiers

27. To enable transactions to be efficiently and accurately traced across the registry system, transactions should be uniquely identifiable through a standard identifier format consisting of fifteen characters:
- A five-character registry identifier of the initiating registry, as defined in paragraph 16 above;

¹ Note that in the AEF, these are referred to as "first ID" and "last ID"

- A hyphen (“-”) separator; and
- A nine digit, zero-padded transaction number that is unique within the initiating registry.

The transaction number is monotonically assigned and is not reused.

The combination of the initiating registry identifier and the transaction number uniquely identifies a transaction across registry systems.

If a transaction is rejected, invalidated, or otherwise not completed, any subsequent attempt to perform the same operation must be assigned a new transaction identifier.

Example

CHE01-000000023	The identifier for a transaction with a number value of 23, initiated by the CHE01 registry.
XMR01-000000999	The identifier for a transaction with a number of 999, initiated by the Article 6.4 mechanism registry.

I. Internet standard date-time stamps

28. The internet standard for timestamps is defined by RFC 3339. This standard is based on ISO 8601 and provides a clear format for representing date and time on the Internet.

The general format for a timestamp in RFC 3339 is as follows:

Component	Format	Description
Date	YYYY-MM-DD	Year, month, and day (e.g., 2026-05-15)
Time	hh:mm:ss	Hour, minute, and second (e.g., 14:30:00)
Time Zone	Z or ±hh:mm	UTC offset (e.g., Z for UTC, -05:00 for EST)

Dates and times are always interpreted in UTC time.

Timestamps should be expressed in UTC time using the internet standard.

Example

2026-05-15T14:30:00Z	represents May 15, 2026, at 2:30 PM UTC
2026-10-10	represents October 10, 2026 UTC

IV. Attributes for primary entities

29. While this document does not recommend schemas for primary entities, it recommends that the primary entities listed below implement the specified attributes to support tracking and validation of compliance with applicable mandates.

A. ITMOs and authorized mitigation outcomes

30. For the purposes of brevity, in this section, the term "ITMO" refers to both of ITMOs and authorized migration outcomes.

1. ITMO unique identifier

31. An ITMO's identifier is composed of an *Originating Party registry Identifier* and a serial number range (*first serial number, last serial number*) as described in paragraphs 23 to 26 above.

2. Cooperative approach identifier

32. The *cooperative approach identifier* attribute references the identifier of the cooperative approach to which the ITMO belongs, as published by the secretariat on the CARP. For A6.4 emission reductions, the *cooperative approach id* is CA0001.

3. First transferring Party

33. The *first transferring Party* identifies the first transferring Party using its Party identifier as described in paragraphs 11 to 13 above. Only participating Parties may be identified as first transferring Parties; therefore, the Article 6.4 mechanism registry ("XMR") is not a valid value for this attribute.

Prior to the first transfer, this attribute has no value assigned.

4. Vintage

34. An ITMO has a vintage year within the range 2021 to 2100, inclusive, which represents the year in which the mitigation outcome underlying the ITMO occurred.

5. Unit type

35. An ITMO has a unit type equal to 1. This attribute is reserved for future use.

6. Authorization

(a) Authorization identifier

36. The *authorization identifier* is a reference to the authorization published by the secretariat on the CARP. Its format is defined in paragraph 15 above.

(b) Authorization version

37. An authorization may be updated after initial registration with the CARP. The *authorization version* attribute identifies the version of the authorization applicable to the ITMO.

7. Is first transferred

38. Upon completion of the first transfer of an authorized mitigation outcome, the *is first transferred* flag is set. An ITMO that has undergone a first transfer must not be subject to another first transfer.

8. Holding registry identifier

39. An ITMO must be trackable. The holding registry identifier identifies the registry currently holding the ITMO. Its format is defined in paragraph 16 above.

9. Holding account identifier

40. An ITMO must be trackable. The holding account identifier identifies the account within the holding registry in which the ITMO is currently held. Its format is defined in paragraphs 18-22 above.

10. Mitigation type

41. An ITMO has a mitigation type of either "Emission reductions" or "Removals". While the cooperative approach under which ITMOs are authorized may have a mitigation type of "Emission reductions and removals", each ITMO block must have a mitigation type of either "Emission reductions" or "Removals".

11. Underlying unit registry identifier

42. The underlying unit registry identifier may identify the registry in which the underlying unit is recorded.

12. Underlying unit first identifier

43. The underlying unit first identifier may identify the first identifier of the underlying unit block in the underlying registry. Where the underlying units are represented as a range of identifiers, this attribute identifies the beginning of that range.

13. Underlying unit last identifier

44. The underlying unit last identifier may identify the last identifier of the underlying unit block in the underlying registry. Where the underlying units are represented as a range of identifiers, this attribute identifies the end of that range. If the underlying unit last identifier attribute is provided, the underlying unit first identifier attribute must also be provided.

B. Transaction**1. Transaction Id**

45. The identifier that uniquely identifies the transaction across any group of interoperating registries. See paragraph 27 for the recommended format of this identifier.

2. From Registry

46. The registry identifier of the registry containing the account from which the ITMOs are transferred. For transactions within the same registry, the from Registry is the same as the to Registry.

3. From Account

47. The account identifier of the account in the from Registry that currently holds the ITMOs. For some transactions within the same registry, such as registration, the from Account is the same as the to Account.

4. To Registry

48. The registry identifier of the registry containing the account that will hold the ITMOs after successful completion of the transaction.

5. To Account

- 49. The account identifier of the account in the to Registry that will hold the ITMOs after successful completion of the transaction.

6. Is First Transfer

- 50. The is First Transfer flag indicates whether the transaction is a first transfer². It is set to true if the transaction is a first transfer and to false otherwise.

7. Transaction Type

- 51. The type of transaction. The Interoperability standards currently use the following transaction types: Registration, Transfer, Use and Cancellation.
- 52. The Interoperability Standards (Annex III, paragraph 3) describe the relationship of these transaction types with the account types described in paragraph 17. Registries opting not to use the Interoperability Standards may leverage the documentation of these relationships to implement transaction validation.

8. ITMOs

- 53. The array of blocks of ITMOs that are the subject of the transaction. Each element of the array represents one block of ITMOs. The array contains at least one element. The blocks of ITMOs specified within a transaction have unique identifiers and must not overlap. All blocks of ITMOs specified within a transaction are held in the same registry account identified by the from Registry and from Account attributes.

9. Status

- 54. Indicates the current status of the transaction, including its final outcome.
- 55. The Interoperability standards use the following status: Proposed, Validated, Invalidated, Accepted, Rejected, Completed, Terminated. A more detailed description of these status, including transition diagrams, can be found in the Interoperability Standards.
- 56. Registries not applying the Interoperability Standards may use this attribute as they see fit but should agree on a set of values with the other registries with which they interoperate.

10. Status Date-time

- 57. The UTC date-time stamp indicating when the transaction status was last changed.

11. Validation Errors

- 58. The Interoperability Standards describe the validations that the Interoperability Hub perform (Annex III of the Interoperability Standards). Registries using the Interoperability Hub may configure some of these validations to generate warnings rather than errors.
- 59. Even if registries opt not to apply the Interoperability Standards, it is recommended that all or part of these validations be applied to transactions to achieve the objectives described in paragraph 5 above.

12. Validation Warnings

- 60. An array of warnings generated as a result of a proposed transaction failing one or more validation checks. Unlike errors, warnings do not invalidate a transaction. Registries are informed of the warnings and may decide whether to continue processing the transaction.

² A first transfer of an ITMO is the first international transfer, unless it is otherwise defined in the ITMO's authorization. See Decision 2/CMA.3 annex, paragraph 2.

13. Labels

- 61. An optional set of registry-defined labels that may be attached to a transaction. Labels are short tags attached to transactions to make it easier to group, search, filter or classify them.

14. External Reference

- 62. External reference information associated with the transaction, such as a contract number.

15. Supplementary Info

- 63. Additional information associated with the transaction that is not captured by other attributes. The content and interpretation of additional information are registry specific.

16. Last Modified Date Time

- 64. The UTC date-time stamp of the last modification to any attribute of the transaction.

17. Creation Date Time

- 65. The UTC date-time stamp of the creation of the transaction in the from registry.

C. Account**1. Account Id**

- 66. The IBAN-conformant identifier of the account, as described in paragraphs 18 to 21 above.

2. Registry Id

- 67. The registry identifier of the registry in which the account is held.

3. Account Type

- 68. The integer value identifying the account type, as described in paragraph 17 above.

4. NDC Start Date-time

- 69. For accounts of type 200 Use towards NDC (see paragraph 17), this attribute contains the UTC date-time stamp indicating the start of the NDC implementation period applicable to the account. Together with the NDC End Date-time attribute, it enables verification that the vintage of an ITMO used towards NDC falls within the applicable NDC implementation period.
- 70. For all other account types, the NDC Start Date-time attribute is ignored.

5. NDC End Date-time

- 71. For accounts of type 200 Use towards NDC (see paragraph 17), this attribute contains the UTC date-time stamp indicating the end of the NDC implementation period applicable to the account. Together with the NDC Start Date-time attribute, it enables verification that the vintage of an ITMO used towards NDC falls within the applicable NDC implementation period.
- 72. For all other account types, the NDC End Date-time attribute is ignored.

6. Labels

- 73. An optional set of registry-defined labels that may be attached to an account. Labels are short tags attached to accounts to make it easier to group, search, filter or classify them.

7. Supplementary Info

74. Additional information associated with the account that is not captured by other attributes. The content and interpretation of additional information are registry-specific.

8. Last Modified Date-time

75. The UTC date-time stamp of the last modification to any attribute of the account.

9. Creation Date-time

76. The UTC date-time stamp indicating when the account was created in the registry.

V. Recommended practices

A. Identification of account subtypes

77. During the elaboration of the communication standards, it was suggested that account type codes in the range 101–199 be used to identify subtypes of 100 holding accounts. Similarly, it has been further suggested that other ranges be used to identify subtypes of other account types. For example, different codes in the ranges, 301–309, 311–319, 321–329 be used to identify different subtypes of cancellation accounts.

The secretariat recommends against this approach for two principal reasons:

- (a) Establishing globally standardized subtype codes would be difficult because registries and regulatory schemes use a variety of account categories and designations for accounts that perform certain functions. Examples for different subtypes of holding accounts include:
- (i) Stationary installation holding account — EU ETS;
 - (ii) Aircraft operator holding account — EU ETS;
 - (iii) Maritime operator holding account — EU ETS;
 - (iv) Regulated entity holding account — ETS2;
 - (v) National holding account — EU ETS;
 - (vi) Entity holding account — Japan’s JCM registry;
 - (vii) Government holding account — Japan’s JCM registry;
 - (viii) Holding account — Australia’s ANREU; and
 - (ix) General account — Verra Registry, which supports the holding and transfer of units, among other functions.

These categories are not necessarily equivalent across registries or schemes, and their definitions and uses may evolve over time.

- (b) Allowing registries to assign their own meanings to codes would undermine the common interpretation of account type codes and could compromise validations based on account type. For example, a transferring Party’s registry and an acquiring Party’s registry might interpret code 150 differently, potentially resulting in inconsistent validation or processing.
78. The secretariat recommends using only account type published in the communications standards (and paragraph 17 above) and using either or both of the following mechanisms to identify registry- or scheme-specific subtypes. Such identification would supplement, rather than modify, the standardized account type:
- (a) Use the labels attribute of an account (see para. 75). Labels are short metadata elements attached to accounts by registries and may be used for grouping, filtering and other identification purposes. A label may identify the subtype under which a registry, or a group of registries, classifies a holding account. For example, registries that have agreed on a common label formatting convention (e.g. a comma-separated type/value pair) could use a label with the type “ACCOUNT_SUBTYPE” and the value “STATIONARY_INSTALLATION” (The label type and value shown here are illustrative and are not prescribed by the communication standards).
- (b) Use reserved ranges within the registry-assigned component of account numbers to identify subtypes of holding accounts. Subject to the account identifier requirements specified in the communication standards and the applicable allocation rules, a registry, or a group of registries, may adopt a convention reserving ranges for particular subtypes.

-
79. The communication standards will not specify validation rules that depend on subtype classifications conveyed through labels or account number ranges. Any requirements governing the structure and validity of labels and account identifiers will continue to apply. Registries are responsible for applying and checking compliance with any classification conventions they have adopted. Adoption of such conventions would not, in itself, ensure a common interpretation across registries.

B. Additional use of account and transaction labels

80. In addition to identifying subtypes of accounts, as described in para. 78, account and transaction labels may be used to classify accounts and transactions for other purposes. For example, registries wishing to identify CORSIA-related transactions could adopt a common labelling convention, such as a label formatted as a type/value pair (comma separated) with the type “SCHEME” and the value “CORSIA”, and apply it to relevant transactions. They could also apply the same label to accounts designated for recording CORSIA-related use or cancellation, provided that the account type is appropriate to the underlying transaction under the communication standards. (The label type and value shown here are illustrative and are not prescribed by the communication standards).
81. Such labelling would facilitate the identification and filtering of relevant transactions and accounts. It would not, in itself, establish the eligibility of individual units for use under CORSIA or demonstrate that those units have been used to satisfy CORSIA obligations.

C. Transaction and data integrity

1. Traceability from mitigation outcomes to ITMOs

82. To ensure complete traceability throughout the lifecycle of mitigation outcomes: from mitigation outcomes to authorized mitigation outcomes, and ultimately to ITMOs, the unique identifier of each mitigation outcome should remain unchanged.
83. Accordingly, when a registry creates a block of mitigation outcomes that have not yet been authorized, it should assign that block a unique identifier in accordance with paragraphs 23 to 26 above.
84. This identifier should be retained when the mitigation outcomes are authorized and should continue to identify the same mitigation outcomes throughout their subsequent lifecycle, including first transfer, use and cancellation.
85. By preserving a single identifier throughout the lifecycle of the mitigation outcomes, an ITMO can be traced directly back to the original mitigation outcome from which it originated, thereby ensuring an unbroken chain of identity and avoiding the need to create, maintain and reconcile multiple identifiers, mapping tables or supporting documents.

2. Reconciliation

86. The guidance in decision 6/CMA.4, annex I, chapter I.B describes the need for “reconciliation procedures within and between registries”.

Reconciliation procedure within a registry

87. Reconciliation within a registry can be achieved by ensuring that the holdings of each account are equal to the cumulative effect of all successfully completed transactions affecting that account. Holdings should be updated as part of the successful completion of each transaction, ensuring that the recorded holdings remain consistent with the transaction ledger.
88. In addition to the real-time updating of holdings, registries should periodically reconcile holdings against the transaction ledger, to verify that no inconsistencies have

occurred. Ideally, such reconciliation would occur in real time, immediately upon the successful completion of each transaction. However, for practical reasons, including the need to maintain acceptable performance when processing large numbers of transactions or managing large holdings, registries may perform full reconciliation on a periodic basis, such as daily.

89. Reconciliation should ensure that the holdings recorded by a registry are consistent with the transaction ledger, including both the quantity and the attributes associated with each mitigation outcome and ITMO. Reconciliation should therefore verify that mitigation outcomes and ITMOs are correctly accounted for using their unique identifiers and that associated attributes, including but not limited to cooperative approach, authorization, vintage, mitigation type and first transfer status, remain consistent throughout their lifecycle.
90. Reconciliation should be performed at a level of granularity sufficient to detect discrepancies in both quantities and attributes. For example, reconciliation based solely on the total number of mitigation outcomes or ITMOs held by a registry or account may not detect cases where units have been incorrectly attributed to another cooperative approach, authorization or other attribute. Accordingly, registries should be able to reconcile holdings and transactions at the level of the relevant attributes and unique identifiers.
91. Where a reconciliation identifies an inconsistency affecting a block of mitigation outcomes or ITMOs, the registry should prevent that block from being subject to further transactions until the inconsistency has been investigated and resolved.
92. The registry should retain a record of the identified inconsistencies and the corrective actions taken

Annex III – Definitions

Account: An account is a partition of a given registry which is used to hold related ITMOs.

API: An Application Programming Interface is a set of rules or protocols that enables software applications to communicate with each other to exchange data, features and functionality.

API operation: An API operation is a specific action that an API allows a client to perform. It typically corresponds to an HTTP request.

API key: An API key is a unique identifier used to authenticate and authorize access to an API

Atomicity: Atomicity is a property of database transactions that ensures that within a set of database operations, either all occur, or none occur.

Authentication: Authentication is the process to confirm the identity of a user.

Authorization: Authorization is the process to verify a permission to do something.

Block: A block is a sequential grouping of consecutive ITMOs.

Broadcast: A broadcast refers to sending a message, event, or data update to multiple recipients or systems at once.

Cipher suite: In TLS, a cipher suite is a set of cryptographic algorithms used to secure communications over a network. It comprises several components, each specifying different aspects of the encryption, authentication, and key exchange processes.

Client: A client is any computer hardware or software device that requests access to a service provided by a server

Concurrency: Concurrency is when two or more events or circumstances occur simultaneously.

Digital certificate: A digital certificate is a file or electronic password that proves the authenticity of a device, server, or user through the use of cryptography and the public key infrastructure (PKI).

Discrepancy: A discrepancy is an unexpected difference. For example, unexpected transactional data or timeouts could be considered discrepancies in a registry system.

First transferring Party: The first transferring Party of a mitigation outcome is the Party that authorizes the mitigation outcome³.

HTTP Basic Authentication: HTTP Basic Authentication is an authentication scheme built into the HTTP protocol. It allows a client to provide a username and password when making a request to a server.

HTTP Client: An HTTP Client is a client that is able to send a request to and get a response from the server in HTTP format.

HTTP Server: An HTTP Server is a type of server responsible for serving or providing web content on the internet or intranet. As a part of a computer network, web servers transfer documents to clients.

GNU: “GNU is an operating system that is free software—that is, it respects users' freedom. The GNU operating system consists of GNU packages ... as well as free software released by third parties.” (from <https://www.gnu.org>)

GNU zip: GNU's version of the zip data compression tool.

Inconsistency: An inconsistency refers to a contradiction or discrepancy between different elements, data, or statements within a system, document, or context.

Interoperability hub: The interoperability hub is a component that tracks and verifies transactions of ITMOs to ensure consistency across connected registries.

ISO 3166-1 alpha-3: ISO 3166-1 alpha-3 are three-letter country codes defined in ISO 3166-1, part of the ISO 3166 standard published by the ISO, to represent countries, dependent territories, and special areas of geographical interest.

ISO 32000-2:2020: ISO 32000-2:2020 is an international standard which specifies what constitutes a well-defined PDF document, how PDF components are constructed and any expected behaviour from software consuming the PDF file.

ITMO: Internationally Transferred Mitigation Outcome. See decision 2/CMA.3, Annex, para. 1.

JSON: JavaScript Object Notation is an open standard file format and data interchange format that uses human-readable text to store and transmit data objects consisting of name–value pairs and arrays (or other serializable values). It is a commonly used data format with uses in electronic data interchange, including that of web applications with servers.

JSON Schema Specification Draft 2020-12: The JSON Schema Specification Draft 2020-12 is a standardized format used to define the structure, constraints, and validation rules for JSON documents.

Key exchange: A key exchange is a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm.

Ledger: A ledger is a set of records used to track transactions, showing debits and credits for different accounts of an organization. It helps to ensure the accounts are consistent and balanced.

Lifecycle management: Life-cycle management, in the context of information technology, is the administration of a system from provisioning, through operations, to retirement.

³ Baku, FCC/PA/CMA/2024/L.15

para. 11: “*Clarifies* ... mitigation outcomes ... if they have been authorized by the first transferring Party”;

para. 12: “*Decides* ..., where the first transferring Party has authorized the use of the same mitigation outcome ...”

Long-term preservation: Long-term preservation refers to the process of ensuring the accessibility, integrity, and usability of digital information over extended periods, typically involving strategies such as migration, emulation, and digital curation.

Manual intervention: A manual intervention is when an operational procedure is performed by hand rather than automatically enacted

Operational procedure: An operational procedure is a documented set of steps or guidelines that detail how a specific task or process should be carried out within the registry system. It provides a structured approach to executing activities, ensuring consistency, efficiency, and compliance with established standards or guidelines.

OpenAPI: The OpenAPI Specification is a framework used by developers to build applications that interact with REST APIs. The specification defines how to communicate with an API, what information can be requested, and what information can be returned.

Originating Party: The originating Party is the Party that owns the registry (the originating Party registry) that registers the authorized mitigation outcomes with the interoperability hub. In most cases, the originating Party is the first transferring Party.

Payload: In the context of data transmission and messaging protocols, a payload refers to the actual data being transmitted, excluding any protocol overhead or metadata.

Sandbox testing environment: A sandbox testing is a non-production environment which allows users to replicate baseline functionality without affecting the related mission critical system.

Private key: A private key is a cryptographic key that is used with an asymmetric (public key) cryptographic algorithm. The private key is uniquely associated with the owner and is not made public. The private key is used to compute a digital signature that may be verified using the corresponding public key.

Receiving account: A receiving account is the destination account to which ITMOs are sent.

Receiving registry: A receiving registry is the destination registry in each transaction.

Reconciliation: Reconciliation, when pertaining to data, refers to the verification checks surrounding the accuracy and consistency of said data.

Registry: A registry is an electronic system used to track, manage, and facilitate the trading of ITMOs. In the context of these interoperability standards, "registry" refers to national registries, including registry sections under the International Registry.

Registry administrator: The term registry administrator refers to the role performed by the individual or individuals nominated by the national focal point of the relevant Party to manage its registry. These individuals may include technical experts.

RFC 1952: RFC 1952 defines the structure and compression algorithm used in GZIP files.

RFC 2119: RFC 2119 defines key words that can be used to signify requirements in each specification and their interpretation.

RFC 3339: RFC 3339 defines a date and time format for use in Internet protocols.

RFC 4180: RFC 4180 defines the format and MIME type for CSV files, which are commonly used for representing tabular data in plain text form.

RFC 8446: RFC 8446 specifies version 1.3 of the Transport Layer Security protocol.

Sending account: A sending account is the origin account from which ITMOs are sent.

Sending registry: A sending registry is the origin registry for a given transaction.

Server: A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network.

Transport Layer Security: Transport Layer Security is a security protocol designed to provide privacy and data security for communications over computer networks, such as the Internet. A primary use case of TLS is encrypting the communication between web

applications and servers, such between web browsers and websites. The current version is TLS 1.3.

Token: A token is a small unit of data representing a particular piece of information or authorization granted to access a resource.

Trusted third party: A trusted third party is an entity which facilitates interactions between two parties who both trust the third party such as a certificate authority.

Unicode: Unicode is a text encoding standard maintained by the Unicode Consortium designed to support the use of text written in the world's major writing systems.

Unix: Unix is a family of multitasking, multiuser computer operating systems characterized by a hierarchical file system, shell-based command-line interface, and support for multitasking.

User-assigned code element: A user-assigned code element is a code at the disposal of users who need to add further names of countries, territories, or other geographical entities to their application of ISO 3166.

Vintage: A vintage is the calendar year in which the mitigation outcomes represented by the ITMO occurred.
