Annex 1

ICCAT IOMS TECHNICAL SPECIFICATIONS

Carlos Mayor[1], Carlos Palma[1]

Forward: This document should be regarded as the preliminary version of the future "*IOMS detailed technical specifications*" document, which will describe in detail aspects such as architecture, development aspects, component interaction, functionality etc. Right now, it has a preliminary structure, a basic description of the architecture, guidelines on development aspects, and the required basic description on functionality. It is intended to be a dynamic document subject to changes as the IOMS project evolves.

1 Architecture

The ICCAT IOMS will be based on open source technologies. Its architecture will have the following features/characteristics:

- Database server: MariaDB 10.3+
- Backend development (server side): Spring Boot, Spring Data Rest, Spring Security, Java 11+
- Frontend development (web clients): Angular 7+, Typescript 3.1+, Nodejs 11+
- Supported web-browsers: Firefox 63+, Chrome 70+, Edge 44+ (Safari 12+)
- Web security: HTTPS (encrypted communication over TSL) with JWT
- Certification: Let's encrypt
- Authentication services: Auth0.com / Okta
- Deployment: Cloud infrastructure (Linux servers)

These features (all together called "the IOMS solution") will be based on micro-services. Through this architecture, each module developed in the application will be a micro-service that can be added, replaced or removed from the solution. This architecture allows a greater decoupling between components which gives a better resistance to errors, faster and easier maintenance, or an increase in scalability. This solution also facilitates (extra benefit) the development of a machine-to-machine communication through the development of a suitable client.

The backend services will be developed using Java technologies including the Spring Framework for database communication over RESTful web services. Specifically, the Spring Boot, Spring Data Rest and Spring Security framework components will be used. This technology was chosen because it is the most mature (testing, stability, fidelity) and the most widely adopted in the Java ecosystem.

Regarding the user interface, a web application developed in Angular 7+ will be used. This technology has been chosen because it is the most widely used (the largest developer community), it is a tested web user interface technology, and its support (documentation, help forums, etc.) is excellent. This technology allows a greater decoupling between the web components and allows for easier maintenance.

The security of the application will use an external authentication provider that will validate the user's authentication. The application will be served over HTTPS (TCL/SSL encrypted communications) using a certificate from Lets Encrypt (https://letsencrypt.org/) authority. The security mechanism will be based on JSON Web Token (JWT). The authentication platform (options in study: Okta or Auth0) is still being studied and decided.

[1] ICCAT Secretariat, Calle Corazón de María 8, 6th floor Madrid Spain

The IOMS database is a relational database which will be developed using MariaDB (https://mariadb.org/) database server engine. This database server (a branch of MySQL) has been selected because of its wide use, its growing yearly trends in adoption and the fact that it is fully open source, thus low cost. The Secretariat has also experience with the use of MariaDB in the development of the SCRS statistical online validation tools (ICCAT forms).

It is necessary to have enough disk space to store the original files correctly sent to/by the IOMS web application. The current IOMS development work, does not yet contemplate the use of a document management software solution. The adoption of an efficient solution (several open-source options are available) to store the IOMS file content needs to be further studied.

2 Hosting

The ICCAT IOMS will be deployed to cloud servers, characterised to have high availability (+99.99%), scalability (on demand power increase/decrease), and security (intranet and extranet high standards), and optionally 24x7x365 technical support. For this, the cloud services of an external provider will be contracted. Although there are many options in the market, ICCAT has already in place a cloud infrastructure (4 Ubuntu Linux cloud servers) deployed in Rackspace. These cloud servers are virtual machines working together within "openstack" ("a cloud operating system that controls large pools of compute, storage, and networking resources throughout a data centre"). This choice facilitates on one hand the growth of the IOMS in times of peak workload and on another hand it simplifies the process of exporting the system to another cloud provider that uses a similar technology.

3 Repository

The code generated in the development of the IOMS will be stored and managed by version-control software. GitLab (https://gitlab.com) will be the track changes software of this project because it is free, open source, reliable and is widely used by developers. One of the biggest advantages of Git is its branching capabilities. Unlike centralized version control systems, Git branches are cheap and easy to merge. This facilitates the feature branch workflow popular with many Git users.

4 Testing

For the development of the IOMS application, three different environments will be created: development, test and production. The test and production environments will be as similar as possible at the database level, directory routes, permissions and versions of the software that runs on it.

The software will be periodically subjected to unit tests in an automatic way that can be programmed with continuous integration systems such as Jenkins.

5 IOMS database

The IOMS database is responsible for storing all the information related to the IOMS system. It is a relational database design model managed by a MariaDB database server engine. A complete backup of the database will be performed once a day, performing several incremental backups throughout the day.

The database structures (tables, relationships, views, etc.) that make up the data model will be continuously modified in the development of the IOMS web platform, so this document must be updated periodically.

The IOMS core database (initial model) consists of the following main tables:

- MessageThread

This table stores the information of communications between a CPC and the ICCAT Secretariat. It must be related to, at least, one message. The table stores the date on which the communication thread was created, the author of that communication thread, the subject and, in the case where it refers to it, the affected requirement.

- Message

This table stores information about the messages exchanged between two users of the system. For the moment it is only thought to be bidirectional between the users of the CPCs and the ICCAT Secretariat. The date and time of the sending is stored, who wrote it and who is the recipient, the thread to which it refers and the address to the folder of attachments in the case in which they have been attached.

- User

This table stores the information of registered users in the system. It will be mandatory to store the contact email information, name, organization to which it belongs and the role assigned in the application.

- Organization

In this table the information of the organizations that will work with the system is stored: CPCs and the ICCAT Secretariat.

- Role

This table stores the information of the roles with which a user can interact with the application. Depending on the role granted, by the administrator users, the user can access one or other views and may execute certain actions.

- Notification

The notification table stores information on all the notifications generated by the system, as well as the notifications generated by the ICCAT secretariat to the CPCs to request information.

- Notification Receiver

In this table, a specific notification is stored, as well as the request to which it refers and the date and time it was sent.

- Requirement

The requirement table stores information on the requirements that are requested from each of the contracting parties in ICCAT. For each of the requirements, the code is stored to identify it, the type of requirement that is involved, a description and a range of dates in which this requirement is valid.

- Recommendation

In this table, all the information of ICCAT resolutions, recommendations and articles is stored. They are identified with a code, their range of dates in which they are active are indicated, a brief summary is described and the URL is stored to refer to the text published on the ICCAT website.

- RequirementRecommendation

This table links the recommendations with their respective requirements.

- DataSubmission

This table stores the data submissions that users have made to satisfy the requirements requested by the ICCAT secretariat. Only correct (after passing through a predefined set of validation rules) data provisions are stored. The date and time of the submission is stored, which user did it, what organization did it, what requirement the sending refers to and the sending information, either in plain text mode, attached files or the electronic form that the user has filled out.

- Eform

This table stores information on the electronic forms published by the ICCAT secretariat to comply with the requested requirements. The code of the electronic form is stored, the form type, the form description and the url of the validator.

- EformRequirement

This table links the electronic forms with the requirements.

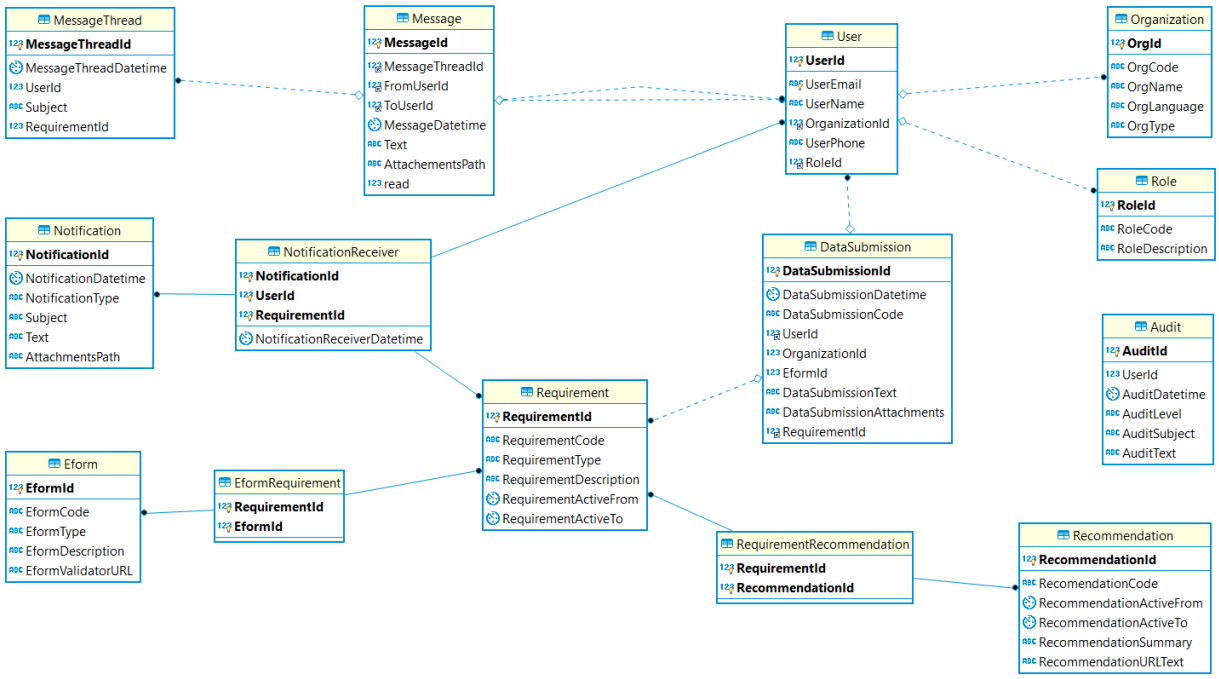

Figure 1 ER (Entity-Relationship) diagram of the IOMS database

6 Modules

6.1 ICCAT web-app platform

a) Security Manager

The module of the security manager will be in charge of controlling whether the user can access the application or not, which views of the application can be seen or add users and roles, for those users who have that permission.

This module consists of several visual components: authentication, login/logout, user registration, cpc-user-list, user-list, user details (profile), roles, and others.

b) Reporting requirements manager

This module is in charge of managing the ICCAT requirements as well as the association with ICCAT regulations (Convention articles, Recommendations, Resolutions, etc.) adopted by the Commission, and, the versioning of the official templates (data in electronic forms, text and other information in explicit templates, others) associated with each one of the requirements on data provision by the CPCs.

This module consists of the following components: requirement-list component, requirement-detail component, recommendation-list component, recommendation-detail component, eform-list component, eform-detail component, cpc-data-list submission component, data-list submission component and data submission details component.

c) Message Manager

This module manages the messages sent between the users of the CPCs and the ICCAT Secretariat. Communications are managed by threads or conversation topics. There may be many messages within each conversation topic and there must be at least one. Currently it is not foreseen to allow

communication between users of the application in which one of them is not the ICCAT Secretariat. The application will allow the sending of attachments with a size limitation. These attached files will not be stored directly in the database but will be stored in a directory structure dedicated to the messages.

This module consists of the following components: cpc-message list component, message-list component, message details component

d) Notification Manager

The notifications management module of the system will be responsible for managing the notifications. In this module you can create a new notification that can be an information request, a system (automatically generated) notification or a warning. Recipients can be selected from this module.

This module consists of the following components: cpc-notification-list component, notification-list component, notification-detail component.

e) Auditing Manager

The audit module is responsible for registering and storing in the database the events generated by the users when interacting with the application. Of special relevance are those events related to the sending of information, the attempts of login in the system or events of special relevance. Only ICCAT administrator users will be able to consult data in this module.

This module consists of the following components: cpc-auditing-list component, auditing detail component.

6.2 *Annual Report Module*

a) Annual Report Part II Section III

This module will manage Annual Report requirement in Part II Section III information. The template that will be used to develop this module is described in the "Revised Guidelines for the preparation of Annual Reports" (Ref.12-13). This module will allow the incorporation of annual changes made by the Commission to the ICCAT reporting requirements. Registered users with the appropriate permissions will complete an online version of the Table in Part II Section III or download a template to fill-out "offline" that can be later uploaded into the system.

A version control manager will be developed as part of this module. This module will show all requirements under the annual report, initially created from the Reporting Requirements Manager component (section 2.1, item 1b) of the IOMS main module.