Qualifications and Credentials Platform

Development Report

ACQF
African Continental Qualifications Framework

Global Gateway

Funded by the European Union

African Union

ETF Working together Learning for life
European Training Foundation

Contents

1. Introduction

This interim development report outlines the progress achieved under Order Form 4 (OF4) for the ACQF Qualifications and Credentials Platform (QCP). It summarises the functional enhancements, technical improvements and operational preparation steps delivered during this period.

The work supports the phased approach defined in the ETF technical specifications, which require the platform to evolve into a fully functional, multilingual, comparable and scalable continental qualifications infrastructure.

1.1. Document Structure

This report is structured as follows:

- **Software Development Status**: describes system development tasks, including backend, frontend, and infrastructure components.
- **Features Delivered**: lists functionalities implemented, such as data entry, user management, and system configuration.
- **Technical Tasks:** details the work done backend services, API development, and deployment configurations.
- **Deployment Status:** describes the infrastructure setup, and platform readiness.
- **URLs and Domains:** Lists relevant platform access points and operational environments.
- **User Roles and Permissions:** Defines roles, access levels, and associated responsibilities.
- **Platform Security:** Explains security measures such as authentication, encryption, and data protection.
- **Next Steps and Recommendations:** Outlines planned improvements, future releases, and long-term sustainability goals.

The sections above reflect the key areas covered in the report, providing a comprehensive view of the platform's technical development progress and the next steps in its implementation.

2. Software Development Status

The platform evolved from a structural prototype into a feature-rich, operational application supporting key functionalities such as virtual space configuration, role-based access management, manual and API-based publication, and real-time validation with KPI monitoring.

By delivering these enhancements, the platform now supports critical use cases for both data entry and bulk publication, aligning with national data workflows and governance models. This marks a major transition toward production-readiness and lays the groundwork for subsequent improvements, including multilingual display, similarity search, and comparison.

Development during this phase was centred on finalising the Import user interfaces and enabling secure backend interactions via authentication and API key management. Public-facing components such as search, filters and qualification details were also introduced and are now available for review and feedback.

2.1. Features delivered

The following key functionalities have been implemented under Order Form 4:

- **Similarity Engine**

[Feature 5.1] Similarity Engine

Core components for identifying *related* qualifications have been implemented. This includes:
• A similarity engine based on structured qualification fields
• Elasticsearch-based similarity search enabling scalable similarity calculations
• Generation of similarity scores to identify related qualifications
• Presentation of similar qualifications within public interfaces

This feature supports discovery of related qualifications and underpins comparability and transparency across national and continental datasets.

- **Duplicate Detection**

[Feature 2.1] Duplicate Detection

Dedicated mechanisms for detecting *duplicate* qualification records have been implemented. This includes:
• Detection of duplicate qualifications based on titles, awarding organisations, and country fields
• Backend and frontend support for duplicate detection during curation and publication
• Integration of duplicate checks into quality-assurance workflows

This feature supports data quality assurance by reducing the risk of publishing overlapping or redundant qualification records.

- **Comparability Tool**

[Feature 5.2] Comparability Tool

The comparability interface for structured comparison across qualifications has been implemented and stabilised. Delivered functionality includes:
• Structured comparison of qualifications across key fields such as level, credits, learning outcomes, and descriptors
• Ability to initiate comparison from search results and qualification detail pages
• Support for comparison of learning outcomes, including skill-based comparison
• Fixes for duplicate entries and layout issues in comparison views
• Improved behaviour and usability on mobile devices

This feature enables transparent comparison across national and continental datasets.

- **Multilinguality**

[Feature 2.13/4.6] Multilinguality

The multilingual foundation of the platform has been implement across curator and public interfaces:
• Support for language selection between English, French, and Portuguese
• Multilingual rendering of qualification details, lists, and curator screens where corresponding data exist
• Handling of multilingual validation and error messages, including accent handling in French and Portuguese
• Support for displaying multiple language variants on qualification detail pages
• Improvements to multilingual sorting and fallback behaviour

These improvements deliver the core multilingual requirements defined for the platform.

- **Integration of Data Model Refinements**

A broad set of refinements requested by countries and ETF has been implemented consistently across backend and frontend. Items include:
• Qualification objective
• Entry requirements
• Volume of learning
• Accreditation dates (registration, expiry, next update)
• Updated accreditation type controlled vocabulary
• Tag indication of qualification type
• Support for decimal credits
• Revised NQF level logic, including support for empty values
• Display and UI adjustments related to ACQF and NQF levels
• Mandatory organisation title enforcement
• Resolution of accreditation versus qualification type inconsistencies

These refinements improve semantic clarity, validation accuracy, and data completeness.

- **Qualification Hierarchy System**

The qualification hierarchy system has been implemented on both backend and frontend and supports:
• Parent–child relationships between qualifications
• Validation preventing circular or invalid hierarchies
• A two-level hierarchy model as agreed with ACQF stakeholders
• Curator-side creation, editing, and release handling of hierarchical links

This feature enables structured qualification representation aligned with ACQF governance decisions.

- **Publication and Validation Improvements**

A number of improvements to publication workflows and validation logic have been completed:
• Refined manual publication behaviour for hierarchical qualifications
• Full application-profile validation when records are set to “ready to publish” or “obsolete”
• Integration of SHACL validation errors into frontend interfaces
• Improved error handling, validation messaging, and curator feedback
• Fixes to release flow, publication reports, and curator regressions
• Corrections to date handling, typeahead fields, rollback behaviour, and form validation

These enhancements support operational stability and national-level bulk publication.

- **Infrastructure and Interoperability Foundations**

The technical foundations needed for interoperability and stable deployment have been strengthened, including:
• Introduction of a functional SPARQL endpoint
• Improvements to backend error handling and internal bug fixes
• Corrections to automated publication administration screens

These steps position the platform for integration with national systems and future automated data exchange.

3. Deployment Status

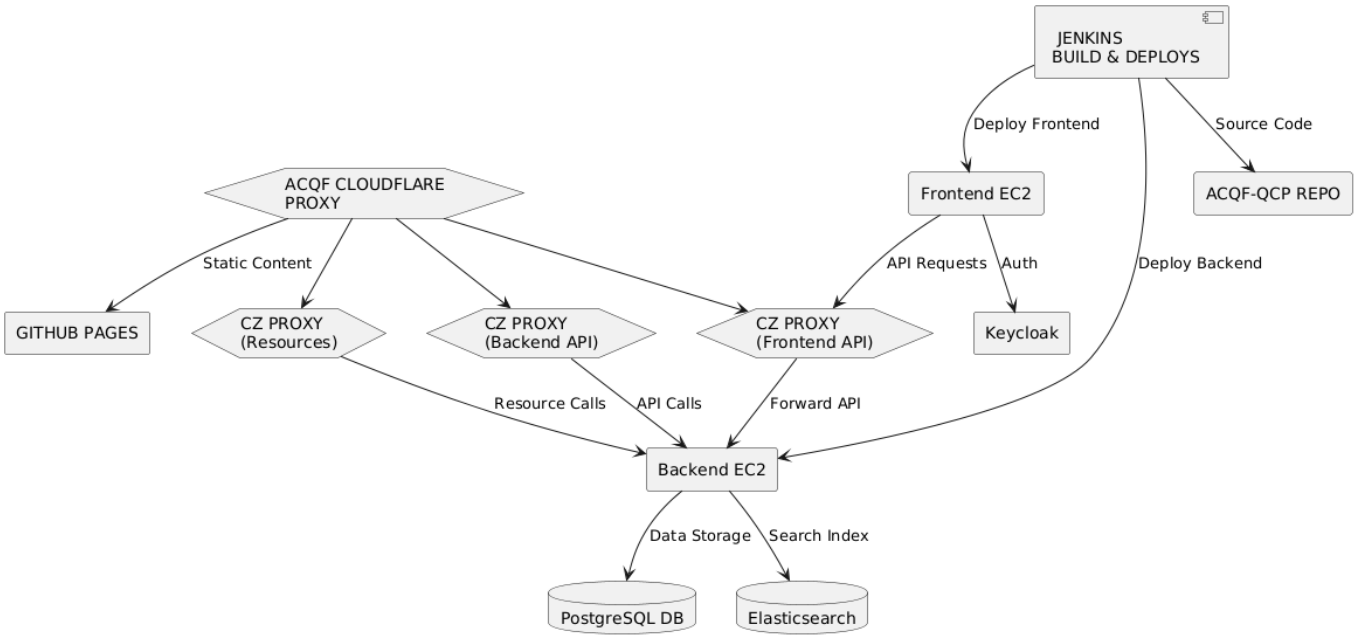
The deployment status remains largely stable involving the necessary infrastructure and domains to host the ACQF QCP, continuously integrate and deliver software to it and make its services available through the web.

The domain acqf-qcp.africa was secured for this purpose.

This activity also detailed the deployment architecture, including the following components

- Cloudflare Proxy
- Cognizone Proxy
- GitHub Pages
- Backend and Frontend EC2 instances
- PostgreSQL database
- Jenkins for CI/CD processes.
- Elasticsearch for data indexing and search optimistation
- Keycloak for aunthentication and authorization services

The deployment setup is designed to ensure efficient traffic routing, robust backend operations, and seamless frontend interactions, providing a reliable and scalable platform for the ACQF QCP.



3.1. Components

- **ACQF Cloudflare Proxy**: Acts as the entry point for external traffic, routing traffic to various subdomains and resources.
- **Cognizone Proxy**: Intermediate proxy layer for routing traffic within the infrastructure, handling traffic to and from backend and frontend EC2 instances.
- **GitHub Pages**: Source for static content deployment, accessible through https://data.acqf-qcp.africa/ .
- **Backend EC2**: Backend server for processing and handling backend operations, connected to the PostgreSQL database for data storage.
- **Frontend EC2**: Frontend server for handling user interface and client-side applications.
- **PostgreSQL DB**: Database server for storing application data, directly connected to the Backend EC2 instance for data operations.
- **Jenkins Build & Deploys**: CI/CD tool used for automating builds and deployments, interacting with the ACQF-QCP repository to deploy updates to Backend and Frontend EC2 instances.
- **ACQF-QCP Repo**: Source code repository containing the codebase for the project, integrated with Jenkins for build and deployment pipelines.
- **Elasticsearch :** Elasticsearch is a distributed, RESTful search and analytics engine designed to provide powerful full-text search capabilities and real-time data indexing for large-scale applications.
- **Keycloak:** Keycloak is an open-source identity and access management (IAM) solution designed to provide authentication, authorization, and single sign-on (SSO) capabilities for modern applications and services.

3.2. Interactions

External Traffic Flow

- Incoming requests from external users are first processed by the **ACQF Cloudflare Proxy**, acting as the central entry point.
- Depending on the request type:
    - **Static Content Requests**: Requests for static resources are routed to **GitHub Pages** through the Cloudflare Proxy.
    - **Backend Operations**: Requests requiring backend logic are forwarded to **CZ Proxy (Backend API)**, which relays them to **Backend EC2**.
    - **Frontend Interactions**: Requests involving the frontend interface are directed to **CZ Proxy (Frontend API)**, connecting to **Frontend EC2** for user interaction.

Internal Traffic Flow

- **Frontend EC2** uses **Keycloak** for authentication and authorization, ensuring secure access to protected resources.
- **CZ Proxy** facilitates internal traffic routing:
    - **Frontend API Requests**: Forwarded from **Frontend EC2** through **CZ Proxy (Frontend API)** to **Backend EC2** for backend processing.
    - **Backend Data Access**: **Backend EC2** performs business logic and communicates with:
        - **PostgreSQL DB** for persistent data storage.
        - **Elasticsearch** for high-performance search and indexing operations.

3. Deployment Flow

- **Jenkins Build & Deploys** automates continuous integration and deployment (CI/CD):
    - It fetches the latest source code from the **ACQF-QCP Repo**.
    - After successful builds:
        - **Frontend EC2** is updated with the latest frontend application code.
        - **Backend EC2** receives updates to backend services, ensuring up-to-date business logic and APIs.

This flow ensures high availability, scalability, and secure interactions while maintaining a modular and optimized deployment process.

3.3. Public URLs

Environment	ACC	PROD
Curator and automated publication URLs	https://curate-acc.acqf-qcp.africa/	https://curate.acqf-qcp.africa/
External public URLs	https://public-acc.acqf-qcp.africa/	https://public.acqf-qcp.africa/

4. User roles

4.1. Administrator

Key Skills and Expertise:

- Strong understanding of all system features, architecture and infrastructure.
- Proficiency in managing cloud-based environments, CI/CD pipelines, and database systems.
- Knowledge of security protocols, such as authentication, encryption, and monitoring tools.

- Technical troubleshooting and problem-solving skills.

Role and Functions:

- Full oversight and management of the platform.
- Configure and maintain backend and frontend services.
- Monitor performance, handle security configurations, and manage user roles.
- Implement updates, patches, and fixes.
- Enforce system-wide policies and resolve any operational issues.

Type of Authorization Needed:

- Full administrative access to all system components, including infrastructure, backend, frontend, and user management.

4.2. Qualification Curator

Key Skills and Expertise:

- Familiarity with data management processes, including CRUD (Create, Read, Update, Delete) operations.
- Understanding of qualification frameworks and organizational structures.
- Basic knowledge of user-friendly content management tools.
- Attention to detail and ability to validate data for accuracy and relevance.

Role and Functions:

- Manage qualification and organization-related data on the platform.
- Create, edit, update, and delete qualifications and organizational records.
- Collaborate with other stakeholders to ensure data consistency.

Type of Authorization Needed:

- Access to CRUD screens for Qualifications and Organizations.
- Restricted permissions to ensure focus on content management only, without access to user or system configurations.

4.3. Virtual Space Administrator

Key Skills and Expertise:

- Intermediate understanding of data and user management.
- Familiarity with role-based access control principles.

- Strong organizational and communication skills for team coordination.
- Attention to security and user-specific access protocols.

Role and Functions:

- Perform all Qualification Curator functions (manage qualifications and organizations).
- Manage user accounts within their specific virtual space, including:
    - Creating and assigning user roles.
    - Modifying access permissions as needed.
- Ensure that the virtual space adheres to data access policies and security standards.

Type of Authorization Needed:

- Access to CRUD screens for Qualifications, Organizations, and Users.
- Role-based access limited to the specific virtual space they administer, preventing overlap or interference with other spaces.

This structure ensures each role operates effectively within its scope, contributing to the overall security and efficiency of the ACQF QCP platform.

5. Platform Security

The ACQF Qualifications and Credentials Platform (QCP) has been designed with a strong focus on protecting the confidentiality, integrity, and availability of stakeholders' data. We understand that ensuring data security is critical to building trust and enabling effective platform adoption. This section explains how the platform safeguards sensitive information through clearly defined measures.

Authentication and Authorization:

- Controlled Access: Each user is assigned specific roles that determine their access level, ensuring that data is only accessible to authorized individuals.
- Role-Based Permissions: Permissions are assigned based on users' responsibilities, limiting access to data and features strictly necessary for their tasks.
- Administrative Management: Designated administrators can manage user accounts, adjust permissions, and revoke access when necessary.

Encrypted Data Transfer:

- Secure Communication Channels: All data transmitted between users and the platform is encrypted using Transport Layer Security (TLS). This prevents interception and ensures data confidentiality.
- Data Integrity Assurance: Encrypted transfers protect against tampering during data exchanges, preserving the integrity of transmitted information.

Data Access Restrictions:

- Virtual Space Isolation: Each organization's data is stored in its dedicated virtual space, fully isolated from other organizations. This prevents data overlap and unauthorized access.
- Fine-Grained Access Control: Access is granted on a need-to-know basis, ensuring that only relevant personnel can access sensitive data.

Data Validation:

- Quality Assurance: Every data entry is checked against strict validation rules to ensure completeness, correctness, and consistency.
- Error Detection and Alerts: The system automatically flags invalid entries, enabling corrective action before data is processed or published.

Vulnerability Watch:

- Security Awareness: The platform maintains a proactive approach to identifying potential vulnerabilities by staying informed of emerging security risks.
- Incident Preparedness: Established procedures ensure that any reported or detected vulnerabilities are assessed and addressed promptly.

These measures ensure that data handled within the ACQF QCP remains secure, private, and reliable. By adhering to industry best practices and implementing strict access controls, we are committed to providing a safe environment for managing and sharing educational and credential data.