This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 776503
- CIRC4Life-H2020-IND-CE-2016-2017/CIRC-2017/TwoStage

A circular economy approach for lifecycles of products and services

Development of Escrow database, Core Brokerage component, security and access control

Deliverable 4.4

PROJECT INFORMATION	
Type of Project	European Commission Horizon 2020
Topic	CIRC-01-2016-2017 Systemic, eco-innovative approaches for the circular economy: large-scale demonstration projects
Grant Agreement No.	776503
Project Duration	01/05/2018 – 30/04/2021 (36 months)
Project Coordinator	Nottingham Trent University (NTU)
Project Partners	Enviro Data (ENV), Jonathan Michael Smith (JS), Kosnic Lighting Limited (KOS), Centre of Research for Energy Resources and Consumption (CIR), European EPC Competence Center GmbH (EECC), The Institute for Ecology of Industrial Areas (IETU), SWEREA IVF AB (SWE), Make Mothers Matter (MMM), ONA PRODUCT (ONA), INDUMETAL Recycling (IND), GS1 Germany GMBH (GS1G), Laurea University of Applied Science (LAU), Center for European Policy Studies (CEPS), Institute of Communication and Computer Systems (ICCS), Recyclia (REC), S.A.T. Alia (ALIA)

DOCUMENT INFORMATION	
Title	Development of Escrow database, Core Brokerage component, security and access control
Version	3.00
Release Date (dd.mm.yy)	28.02.20
Work Package	WP4
Dissemination Level	PU

DOCUMENT AUTHORS AND AUTHORISATION	
Document Responsible	Georgios Tsimiklis, ICCS
Contributors	Miltos Koutsokeras , ICCS Sten-Erik Bjorling, ENV
Reviewed by	Georgios Tsimiklis
Approved by	Professor Daizhong Su (NTU)

DOCUMENT HISTORY			
Version	Date (dd.mm.yy)	Description	Implemented by
1.00	20.02.20	First draft	ICCS with the contribution of all stakeholders
2.00	21.02.20	First Internal Review	ICCS
3.00	25.02.2020	Incorporated ENV input and review	ENV, ICCS

Summary

This report document contains the outcome of the following Tasks:

- **Task 4.3: Core Access, Privacy & Security Management.** A central Access Control Manager (ACM) component is deployed for the protection of private data and services plus the authentication and authorisation procedures. All services provided by the ICT Platform are integrated with this ACM and EU General Data Protection Regulation (GDPR) is respected throughout all applications integrating with the ACM.
- **Task 4.5: Core Services Specification & API Development for External Systems & Solutions Access.** A list of RESTful API Web services are created to implement the ICT platform core node functions: Eco-credits calculation (described in Deliverable 2.4), Eco-account and Shopping for consumer client applications, EPCIS-based traceability tool (Task 5.2) integration and retailer applications integration.
- **Task 4.6: Products Eco-points & Escrow Database Development & Implementation.** A database that plays the role of the main repository/escrow system for product data and information.

All technical details on the implementation and usage of the ICT Platform and external systems, are deployed in a website portal found at: https://circ4life.iccs.gr/. The portal is used by all involved partners in order to check progress on implemented components and consult usage, technical documentation and examples. This document provides the credentials for the reader to access the descriptions of the underlying technology, the source code of the development as well as instructions on how to replicate the ICT Platform, everything found in the online address mentioned above.

Table of Contents

Acronyms and abbreviations

Abbreviation	Description
ACM	Access Control Manager
GDPR	General Data Protection Regulation
JSON	JavaScript Object Notation
ICT	Information Communication Technology

1 Introduction

1.1 CIRC4Life ICT Platform Web Services

The **CIRC4Life ICT Platform** is the main host system of the **Access Control Manager** (ACM), the **RESTful API Web Services** and **Persistent Databases** including user Eco-accounts and Master Product Data information. End-users and client applications retrieve and update data by using the single authorization point provided by the integrated ACM. All data flows from and to the ICT Platform are protected by the ACM and communication is always made on top of encrypted **Hypertext Transfer Protocol Secure (HTTPS)** protocol. The current stable and public deployment is reached at **circ4life.iccs.gr**, which also hosts the portal with system and development information mentioned in the summary. The system is compliant to GDPR guidelines.

1.2 Escrow Database

The escrow system allows for long-term storage of a large number of different types of information and data connected to a specific product, resource, method, process or other entity, including future types of information that currently cannot be fully defined. Information types covered in the CIRC4Life implementation are product basic data, input and results data for PEF / LCA calculations, interconnectivity with traceability routines, multimedia types and information types covering ecoPoint / ecoCredits calculations. The core functionalities of the escrow system support data entry, management of the interoperability system in CIRC4Life, thus saving development time and increase flexibility.

2 CIRC4Life ICT Platform Web Services

The ICT Platform is the host system of the **Core Access, Privacy & Security Management** mainly via the Keycloak ACM and the **Core Services API implementation** via a list of custom Java Platform Enterprise Edition modules created by ICCS. The approach used is a **Service Oriented Architecture** where a standardized OpenAPI specification of all available Core Service API endpoints are described in a high level, allowing client application developers to quickly integrate the provided services using various technology stacks and solutions.
All technical details are deployed in a portal also hosted by the ICT Platform system, reachable at https://circ4life.iccs.gr/. The portal is protected by ACM also, to avoid malicious access to valuable development details and block web crawlers' access. The reader of this document can access the portal with a guest account created on the ACM for this specific purpose:

The portal was created for internal usage by all involved partners and this document is the first public availability of all included information. In summary the portal contains:

- OpenAPI and WADL specifications: https://circ4life.iccs.gr/AppsICTPlatform/OpenAPI.html
- Developer documentation: https://circ4life.iccs.gr/AppsICTPlatform/Documentation.html
- Data models: https://circ4life.iccs.gr/AppsICTPlatform/DataModels.html
- ACM and RESTful API Service usage: https://circ4life.iccs.gr/AppsICTPlatform/Usage.html
- Changelog and Road map: https://circ4life.iccs.gr/AppsICTPlatform/Changelog.html

The ICT Platform system and the technical documentation portal (https://circ4life.iccs.gr/) will be available during the lifetime of the CIRC4Life project, plus an additional period of 18 months after the project is concluded.

2.1 Access Control Manager

The ACM is responsible for all Authentication and Authorization of the ICT Platform. It handles the consumer's Eco-accounts and the accessibility of 3rd party application to the provided RESTful API Web Services. The implementation is based on the Open Source Identity and Access Management platform Keycloak, a project supported by the industry's open source leader RedHat. Keycloak uses standard protocols and provides support for OpenID Connect, OAuth 2.0, and SAML. It integrates with a large list of different technology stacks and programming languages via Client Adapter libraries. It can federate user repositories from external LDAP or Active Directory servers and also provides identity brokering for external social networks (**not** implemented currently in ICT Platform) including:

- OpenID
- Facebook
- Google
- Twitter
- GitHub

The ACM server is deployed at https://circ4life.iccs.gr/auth/ and automatically handles all integrated applications via a list of trusted registered applications. The client application registration is maintained by ICCS via the ACM configuration. Any registered client application has two methods to get authorization:

- OpenID Connect
- EndUserModule Eco-account RESTful API service endpoints

The applications that wish to access ICT RESTful endpoints should use the OpenID Connect workflow. In summary this workflow is performed by getting the contents of the OpenID Connect Discovery URL and using HTTP requests on the described endpoints. The authentication of a client application is performed by providing the registered client identification and valid credentials. The client identification and credentials are created by the ACM administrator and shared with trusted developer teams. Then a client can request for an authorization secret token and use it to access all protected RESTful endpoints. This effectively removes the authentication and authorization implementation from each Web Service and moves it to the central ACM service. Once a client is revoked from ACM, all access is forbidden on integrated services.

Here is the workflow in steps:

1. The ACM Administrator registers the configuration of a specific client application, defining the **Client ID** and **Credentials** (username, password). These are all private and shared with trusted developers of the client application.
2. The client software downloads the OpenID Connect Discovery URL document in order to get the required ACM authorization token endpoint (**token_endpoint**).
3. Request from the authorizaation token endpoint to return access tokens that allow access to protected resources (in our case the RESTful API endpoints). The access tokens have a predefined expiration period and cannot be used forever. Client applications should refresh them accordingly with new requests to ACM authorization token endpoint.
4. Use the access token in every request performed on protected resources. Valid and not expired tokens will be accepted.
5. Optionally, the client application can end the authorization session by using the access tokens on a request to ACM session termination endpoint (**end_session_endpoint**).

For convenience, consumer facing end-user applications (e.g. mobile device native applications) can use a simplified user session API provided by the ICCS implemented EndUserModule RESTful Web Service.
All communication between the clients and ACM and protected resources is performed with the HTTPS protocol, effectively encrypting the traffic and protecting from man-in-the-middle attacks. The process above is the back-end of all user authentication and authorization, even for front-end user interfaces that use the typical login form and logout actions. All end-user base identification (**username, password, email, firtname, lastname**) is contained within a single database inside the ACM. Additional information should be kept on application specific databases.
The complete documentation in full detail on how to use the ACM is described in the ACM and RESTful API Service usage page: https://circ4life.iccs.gr/AppsICTPlatform/Usage.html. This page also contains examples to test the behaviour of the ACM prior to development. We avoid duplicating the same content here.

2.2 RESTful API Web Services

The ICT Platform specifications described in Deliverable 4.1 are implemented by these RESTful API Web Services:

- **EcoCreditCalculatorWS**:The ICT Platform Web Service that exposes the EcoCreditCalculator library functionality via a RESTful API. The EcoCreditCalculator library implements the Eco-credit calculation for products as described in **Deliverable 2.4: Eco-credits method final definition**.
- **EndUserModuleWS**: The ICT Platform Web Service for the 4.1 Eco Account and Shopping Module integration via a RESTful API. This module is the back-end of the CIRC4Life mobile application and allows the registration and usage of consumer Eco-accounts.
- **RecycleModuleWS**: The ICT Platform Web Service for the Recycle/Reuse Module and Traceability Web Application integration via a RESTful API.
- **RetailerModuleWS**: The ICT Platform Web Service for the Retailer Module integration via a RESTful API.

The complete reference of the RESTful API specification is described in the ICT Platform REST Web Services API page. This page contains links to OpenAPI version 3 specifications of the available endpoints and input/output data models for requests/responses respectively. The OpenAPI specification files are authored using the YAML human friendly data serialization standard and commented according to user and system requirements:

- **Common definitions** used by all services: CommonOpenAPI.yaml
- **EcoCreditCalculatorWS**: EcoCreditCalculatorOpenAPI.yaml
- **EndUserModuleWS**: EndUserModuleOpenAPI.yaml
- **RecycleModuleWS**: RecycleModuleOpenAPI.yaml
- **RetailerModuleWS**: RetailerModuleOpenAPI.yaml

The complete documentation in full detail on how to use the RESTful API Web Services is described in the ACM and RESTful API Service usage page: https://circ4life.iccs.gr/AppsICTPlatform/Usage.html. This page also contains examples to test the behaviour of the ACM prior to development. We avoid duplicating the same content here.

2.2.1 Source Code

The source code and build instructions in details are available in the ICT Systems Source code page: https://circ4life.iccs.gr/AppsICTPlatform/SourceCode.html.

2.3 Persistent Databases

The persistent storage of the ICT Platform consists mainly of a list of MongoDB databases, containing "unstructured"/dynamic data in JSON representation. On these schema-less databases, the linked relationships between them and external sources is designed with the W3C recommendation, JSON-LD. JSON-LD is a Linked Data format initiative, aiming towards the transformation of WWW to the Semantic Web. The major characteristic is the creation of links between information and the standardization of common properties using shared vocabularies/ontologies like Schema.org, openLCA and GS1 Vocabulary from GS1 SmartSearch.
The ICT Platform contains the following databases:

- **Products Master Data**: Product information records using the Schema.org defined classes, Product and IndividualProduct.
- **User Eco-account Data**: Eco-account information records using the Schema.org defined class Person, plus a custom Eco-balance record coupled with the Person that holds the Eco-points and Eco-credits of the end-user and his history of purchases and recycled items.

The complete documentation in full detail on the data structures used for storing and exchanging information between system components is described in the Software Data Models and Persistence Layer page: https://circ4life.iccs.gr/AppsICTPlatform/DataModels.html.

2.4 General Data Protection Regulation Compliance

The GDPR compliance of the CIRC4Life software ecosystem is a collaborative effort, between the project technical partners. Everyone involved in the project's software development has consider by design principles of data privacy and protection. In the following section we describe the GDPR compliance requirements and how the project's software and process implement them.

2.4.1 Obtaining consent

All end-user should agree on a clear list of terms, provided to them mainly during account registration. The terms of usage conditions must be clear and not use complex language that may confuse the end-users. Also, the consent must be easily given and withdrawn whenever the user wishes.
Since the ICT Platform is the back-end and does not have direct communication with end-users, there is no terms or conditions agreement functionality. End-user facing application like the CIRC4Life mobile applications, presents this information to end-users. This requirement is the responsibility of end-user client applications.

2.4.2 Timely breach notification

In case the system security is breached from a malicious attack or software malfunction, the system administrators must report the incident to end-users and any partner using the service within 72 hours.
This is an aspect that is under consideration, since the ICT Platform and other public systems, do not have a 24/7 monitoring responsible IT team allocated on the systems. All systems are prototypes developed for the project demonstration needs and proof of concept scenarios. ICCS have deployed a full logging and monitoring functionality on all ICT Platform processes and will inform as soon as possible all interested parties in case of a breach.

2.4.3 Right to data access

All end-users should have access to their full account profile and all related data as an electronic copy of the data collected about them. There should be also a report of the usage of account profile data.
The ICT Platform EndUserModuleWS Web Service contains an endpoint which returns the full electronic record and user action history: **/ecoaccount/user_record** endpoint allows to properly logged in users to download a full copy of their Eco-account record in JSON format. The response is easily read by humans and machines alike and contains everything the ICT Platform knows about a specific end-user. This record is also what is deleted forever when the end-user decides to perform a resignation of the system.

2.4.4 Right to be forgotten

All end-users should have the right to request the erasure of their complete record and personal data from the system. This is also known as the right to **Data Deletion**.
The ICT Platform EndUserModuleWS Web Service contains an endpoint for Eco-account resignation: **/ecoaccount/resignation**. This endpoint allows to properly logged in users to effectivelly delete their full Eco-account record from the system. All personal data and actions (shopping, recycling) are removed forever from the ACM and RESTful API services back-end databases.

2.4.5 Data portability

This is a requirement very closely related to the **Right to data access**. The end-users should be able to reuse their data copy if a different environment.
The ICT Platform provides all data responses as JSON documents. JSON is a lightweight data-interchange format, it is supported and integrated in a wide variety of technology software stacks and can be easily parsed from machines, while being human readable.

2.4.6 Privacy by design

This requires that all system and data exchanges are performed using proper security protocols across all components involved.
The ICT Platform use a state of the art Access and Control Manager with Keycloak and all data communications are on top of the latest secure layer of HTTPS. All systems involved are kept up to date with software patches and operating system updates. System Design approach has considered a secure and private environment between all components, server and client processes.

2.4.7 Potential data protection officers

This requirement is optional and depends on the nature and size of the organizations deploying the software solutions. The appointment of an expert person as Data Protection Officer (PDO) depends on the size of the deployed solutions, their purpose and the methodologies used for collecting and processing the data.
The CIRC4Life project GDPR aspects are monitored via the project's Data Management Plan, which is under the responsibility of the project coordinator Nottingham Trend University. The corresponding Deliverables are:

- **D10.2: Data Management Plan - #1**
- **D10.3: Data Management Plan - #2**
- **D10.4: Data Management Plan - #3**

3 Escrow Database

3.1 Description

The escrow system allows for long-term storage of a large number of different types of information and data connected to a specific product, resource, method, process or other entity, including future types of information that not fully can be defined at this time. Information types covered in the CIRC4Life implementation are product basic data, input and results data for PEF / LCA calculations, interconnectivity with traceability routines, multimedia types and information types covering ecoPoint / ecoCredits calculations. The core functionalities of the escrow system support data entry, management of the interoperability system in CIRC4Life, thus saving development time and increase flexibility.

The escrow system is developed using Omnis Studio and PostgreSQL. Omnis Studio is a development environment allowing for parallel management of database, services access & hosting, design of end-user systems for desktop computers, web browsers and mobile devices. The system can be implemented on Linux (server only), Windows and MacOS – all allowing scalability between servers both on application server layer and on database server layers.

The components needed for an initial install (more extensive installs demanding more advanced servers) demand additional resources dependent on local implementation variants. The installation instruction below covers a local installation for testing and access to the systems overall source code.

3.2 Source code

The source code and build instructions in details are available in the ICT Systems Source code page:
https://circ4life.iccs.gr/AppsICTPlatform/SourceCode.html