Co-funded by the Horizon 2020
Framework Programme of the European Union
Grant Agreement Number 825532

Large-scale EXecution for Industry & Society

www.lexis-project.eu

IMPLEMENTATION OF OPAQUE TOKENS FOR IRODS - KEYCLOAK OPENID SOLUTION

WORKSHOP ON CLOUD STORAGE SYNCHRONIZATION AND SHARING SERVICES COPENHAGEN, 27-29 JAN 2020

RUBÉN JESÚS GARCÍA-HERNÁNDEZ (1),
MARTIN GOLASOWSKI (2)

(1) BAdW-LRZ, (2) IT4Innovations

INTRODUCTION

Technologies

- OpenID
  - Open standard and decentralized authentication protocol
- Keycloak
  - Open source Identity and Access Management solution
  - Single-Sign On, Identity Brokering and Social Login, User Federation, Client Adapters
  - Admin Console, Account Management Console, Standard Protocols, Authorization Services
- iRODS
  - The Integrated Rule-Oriented Data System is open source data management software
  - Aimed at deployment in mission critical environments
  - Virtualizes data storage resources
  - Supports microservices, storage systems, authentication, networking, databases, rule engines, and an extensible API

PROBLEM STATEMENT

High-level description

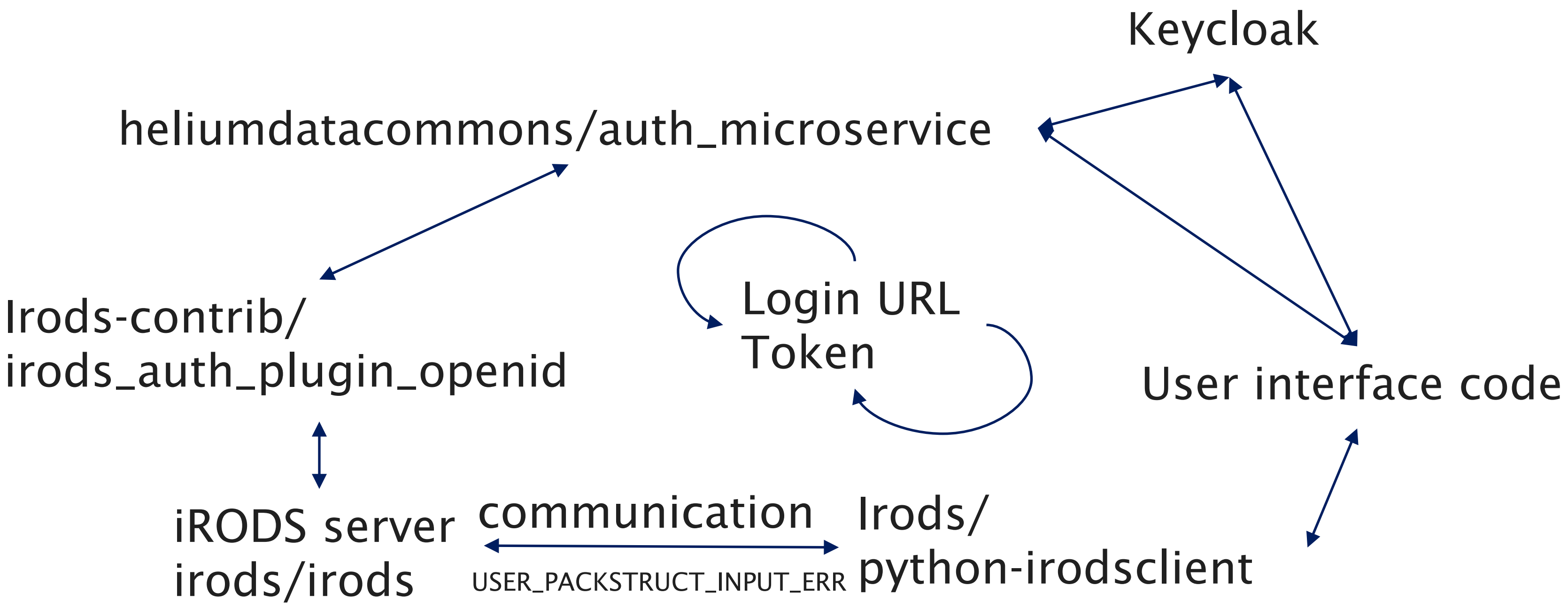
- The standard solutions for iRODS OpenID authentification send tokens using the username field
- This username field has a maximum length of 1024+64 bytes

- Keycloak provides non-opaque JWT tokens with extensive information, with signature. Tokens exceed the length mentioned above
  (typical: 1200 bytes, up to 65000 bytes)

- The iRODS / Keycloak combination, due to the issue above, produces an iRODS error when the token is sent from client to server: USER_PACKSTRUCT_INPUT_ERR

PROBLEM STATEMENT

Diagram



Keycloak

heliumdatacommons/auth_microservice

Irods-contrib/
irods_auth_plugin_openid

Login URL
Token

User interface code

iRODS server
irods/irods

communication

USER_PACKSTRUCT_INPUT_ERR

Irods/
python-irodsclient

SOLUTIONS

- Depending on whether the user is available or not:

A) For web-based applications interfacing directly with the user

- Use parallel execution to perform the query in the background,
- While the user is led through the authentification
- Send the data to the user once it is gathered.

B) For back-end applications, the solution above is not applicable.

- Implement opaque tokens in microservice by accepting a hash of the token.
- Pre-authorize the token by talking to microservice before submitting to iRODS.
- Optimization: hash token in iRODS libraries if >1024 bytes.

CONTACTS

Rubén Jesús García Hernández (LRZ)
garcia@lrz.de

Martin Golasowski (IT4I)
martin.golasowski@vsb.cz

Large-scale EXecution for Industry & Society

LEXIS

CONSORTIUM

VSB TECHNICAL UNIVERSITY OF OSTRAVA | IT4INNOVATIONS NATIONAL SUPERCOMPUTING CENTER

GFZ Helmholtz Centre Potsdam

ITHACA

cea

Avio Aero A GE Aviation Business

EIFFAGE TESEO

Bull atos technologies

lrz Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschafter

cima RESEARCH FOUNDATION

ISMB Istituto Superiore Mario Boella

SECLUDIT AHEAD OF SECURITY

CYCLOPS

ECMWF

AWI

BAYNCORE LABS

NUMTECH L'ATMODÉLISATION