A light-weighted authentication mechanism for IVOA standards

C.M. Zwölf

Victoria Interop, May 2018

Introduction

- Add an authentication level to existing services implemented using IVOA standards
    - The solutions should work both in script & graphical interactive mode
    - Typical targeted services: TAP and UWS
    - Add the authentication without "braking the existent"

The proposed architecture

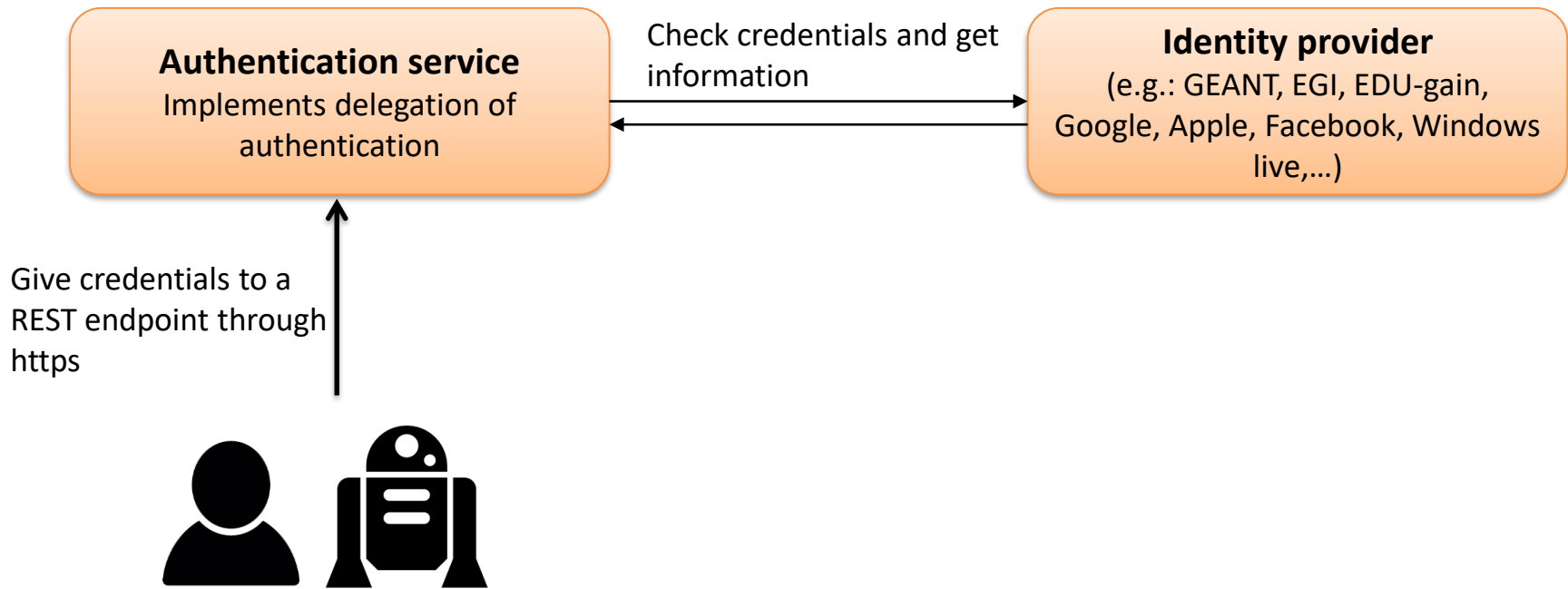**Authentication service**
Implements delegation of authentication

Identity provider
(e.g.: GEANT, EGI, EDU-gain, Google, Apple, Facebook, Windows live,…)

The proposed architecture

Authentication service
Implements delegation of authentication

Identity provider
(e.g.: GEANT, EGI, EDU-gain, Google, Apple, Facebook, Windows live,…)

Give credentials to a REST endpoint through https

The proposed architecture

Authentication service
Implements delegation of authentication

Check credentials and get information

Identity provider
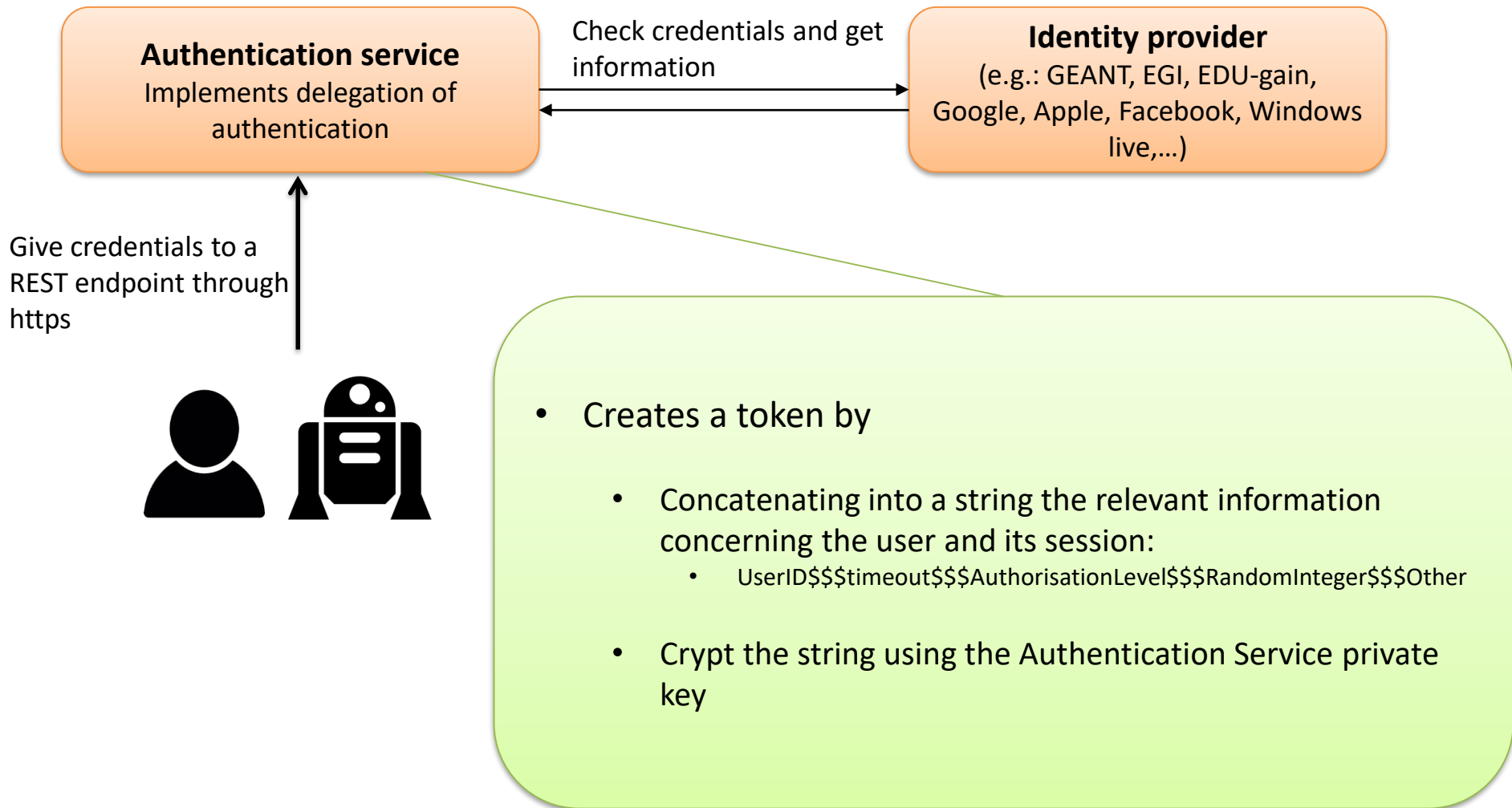(e.g.: GEANT, EGI, EDU-gain, Google, Apple, Facebook, Windows live,…)

Give credentials to a REST endpoint through https

The proposed architecture

Authentication service
Implements delegation of authentication

Check credentials and get information

Identity provider
(e.g.: GEANT, EGI, EDU-gain, Google, Apple, Facebook, Windows live,…)

Give credentials to a REST endpoint through https

- Creates a token by

  - Concatenating into a string the relevant information concerning the user and its session:
    - UserID$$$timeout$$$AuthorisationLevel$$$RandomInteger$$$Other

  - Crypt the string using the Authentication Service private key

The proposed architecture

Authentication service
Implements delegation of authentication

Check credentials and get information

Identity provider
(e.g.: GEANT, EGI, EDU-gain, Google, Apple, Facebook, Windows live,…)
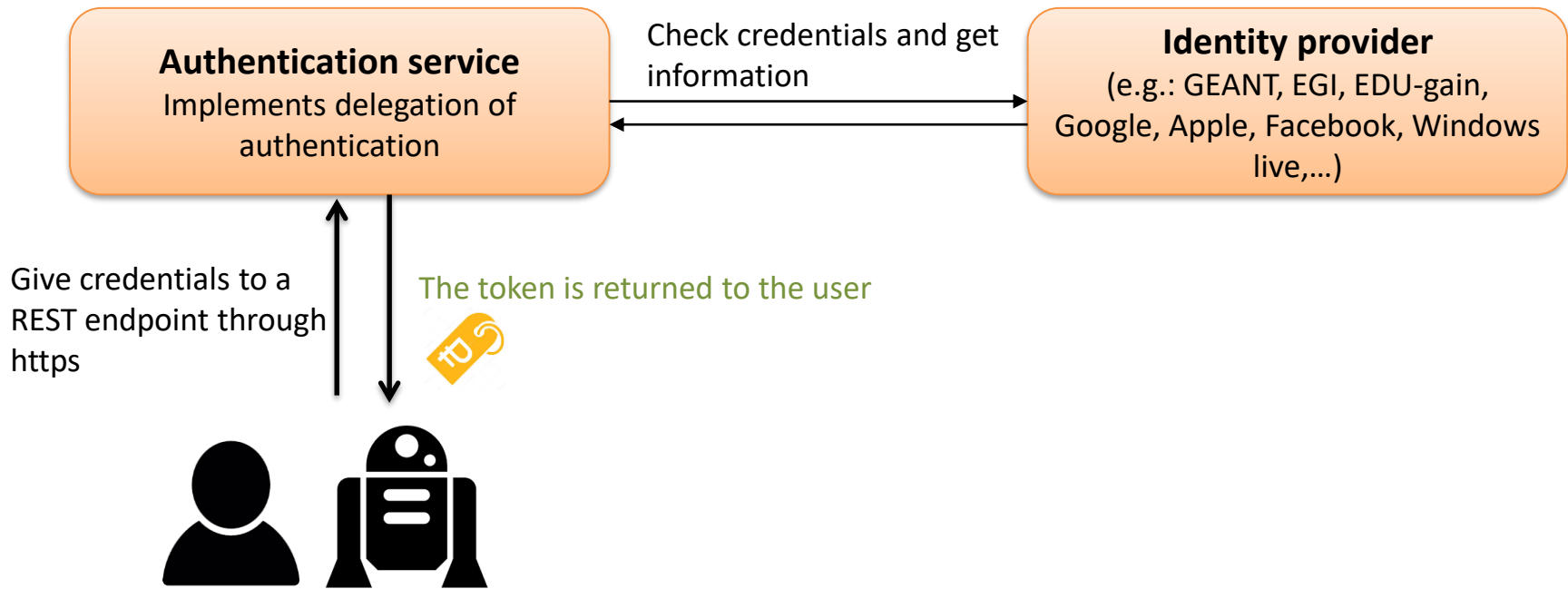
Give credentials to a REST endpoint through https

The token is returned to the user
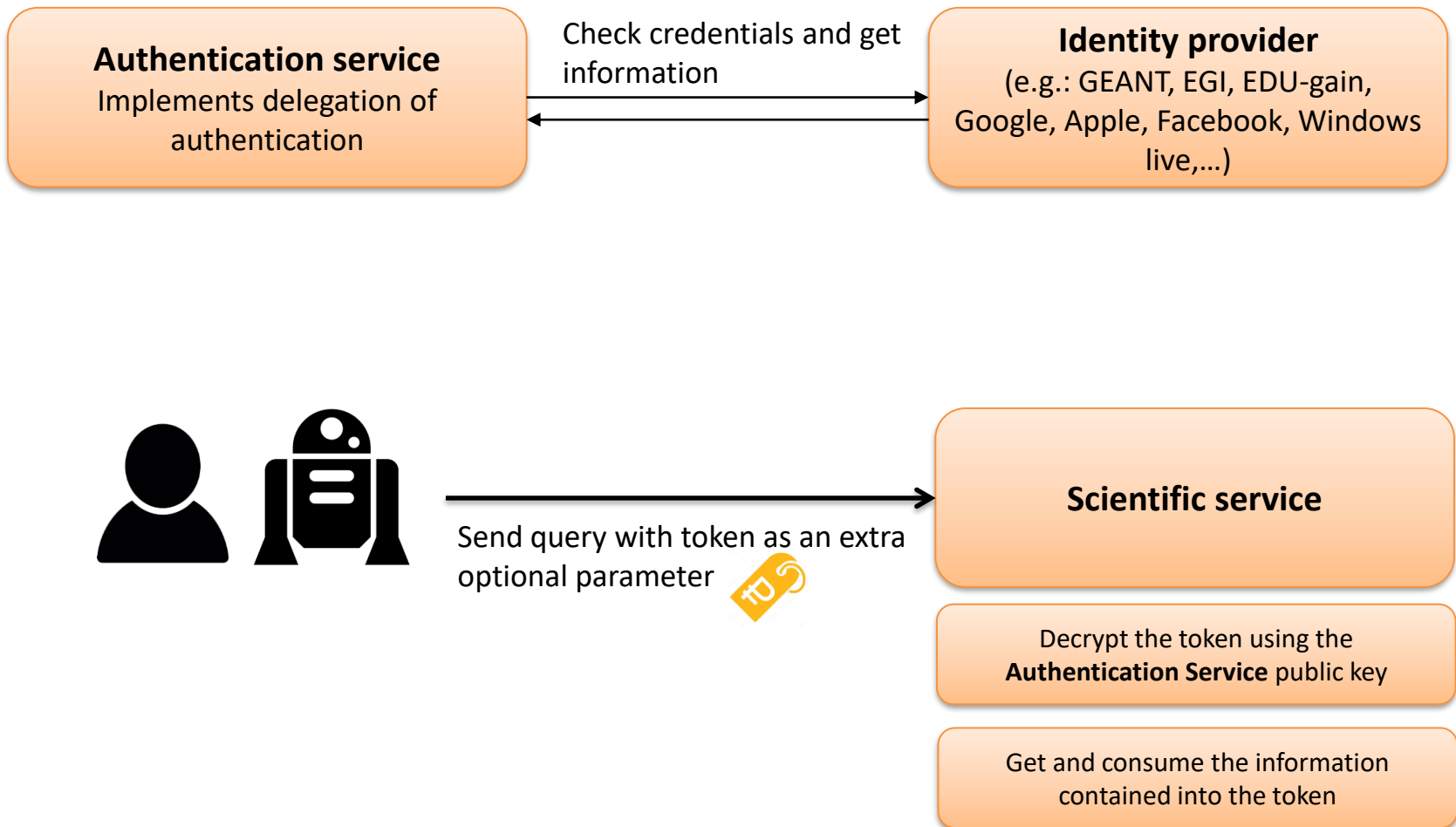
The proposed architecture

Authentication service
Implements delegation of authentication

Check credentials and get information

Identity provider
(e.g.: GEANT, EGI, EDU-gain, Google, Apple, Facebook, Windows live,…)

Send query with token as an extra optional parameter

Scientific service

The proposed architecture

Authentication service
Implements delegation of authentication

Check credentials and get information

Identity provider
(e.g.: GEANT, EGI, EDU-gain, Google, Apple, Facebook, Windows live,…)

Send query with token as an extra optional parameter

Scientific service

Decrypt the token using the **Authentication Service** public key

Get and consume the information contained into the token

The proposed architecture

Authentication service
Implements delegation of authentication

Check credentials and get information

Identity provider
(e.g.: GEANT, EGI, EDU-gain, Google, Apple, Facebook, Windows live,…)

Send query with token as an extra optional parameter

Scientific service

Each service is able to validate and consuming a token → no bottleneck

A given token (as long as it is not out-of-date) may be piped from one service to another → Trivial to script automatic processing supporting authentication