A novel and modern Authentication method for FDSN web services

Javier Quinteros, Rob Casey, Jerry Carter, Elisabetta D'Anastasio, Jonathan B. Hanson, Florian Haslinger, Helle A. Pedersen, Jonathan Schaeffer, Angelo Strollo, Lesley Wyborn and the EIDA Technical Committe

Why do we need to authenticate?

- The first reason is always **because there are restricted data**.
- However, this is important for authorization, not authentication.

- Authentication checks who a person is.
- Authorization checks which specific resources a user has access to.

- To understand usage patterns is fundamental to improve services.
- It could also improve the quality of our statistics.
- It allows our funders to understand the impact of our data and services.

FDSN current standard

- Only the dataselect web service has the option to be used with authentication. EventWS and StationWS don‘t have authentication.
- In dataselect there is a „queryauth“ method to authenticate and submit a data request.
- We have 2 methods to get data: query and queryauth.
- HTTP Digest Authentication (RFC 2617) should be requested from the client.
- Authentication credentials are data center specific.

Limitations

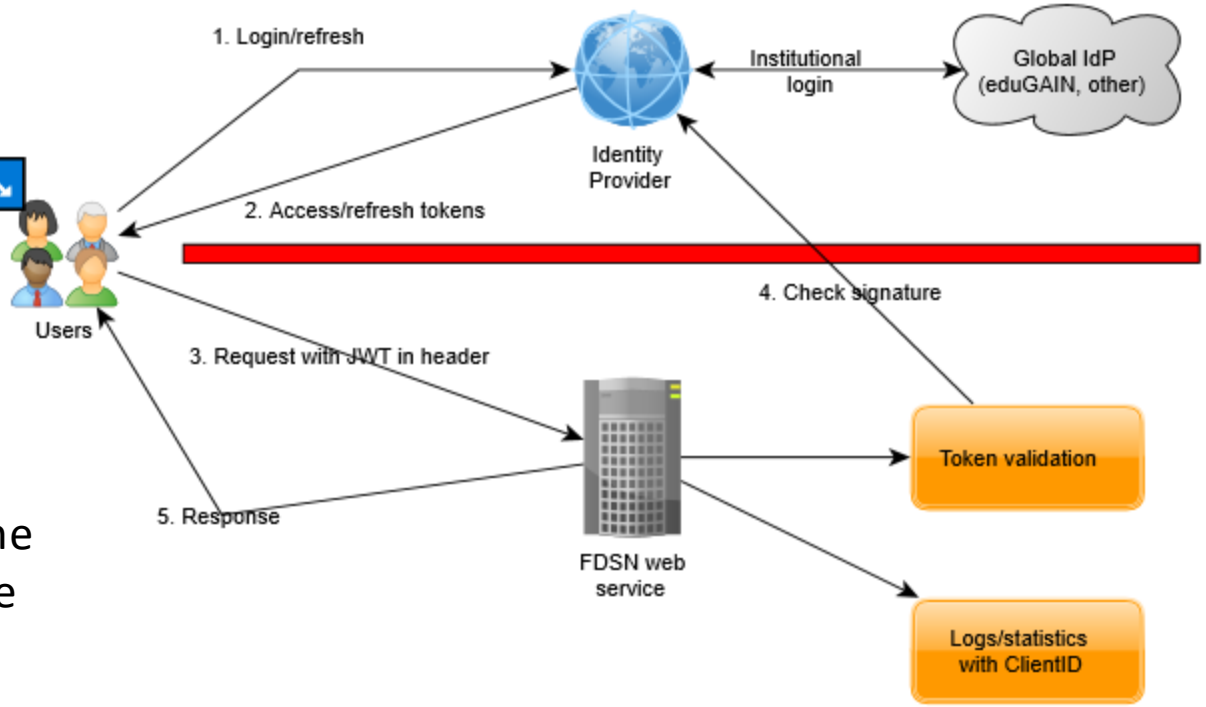
- Implementation uses the “HTTP Digest Authentication” (RFC 2617).
- Only a couple of WS allowed Authentication.
- Authentication credentials are data center specific.
- It cannot be used with many other services apart from some HTTP APIs.
- Users have to register at all data centres, and keep track of all usernames and passwords.
- Not a good solution to support a federation of data centres.
- The only workaround would be to synchronize user databases between data centres, what is extremely dangerous and is discouraged.

Challenges of Federated Authentication

- Services supporting open/embargoed data.
- Thousands of users/year around the world. Most of them unknown.
- New regulations on privacy (GDPR).
- Avoid the need to manage sensitive data at the data centre.
- Foster user authentication for open data (better statistics).
- Better understanding of how data is being used.
- How to properly manage a user database?

OAuth2: The protocol

- **Approach**: Decouple from user login ➡ and service provisioning ↘
- User receives a token and presents it to the service providing data.
- The eduGAIN initiative (>8000 institutions) allows users to log in at their home institutions. We don't store any user data!

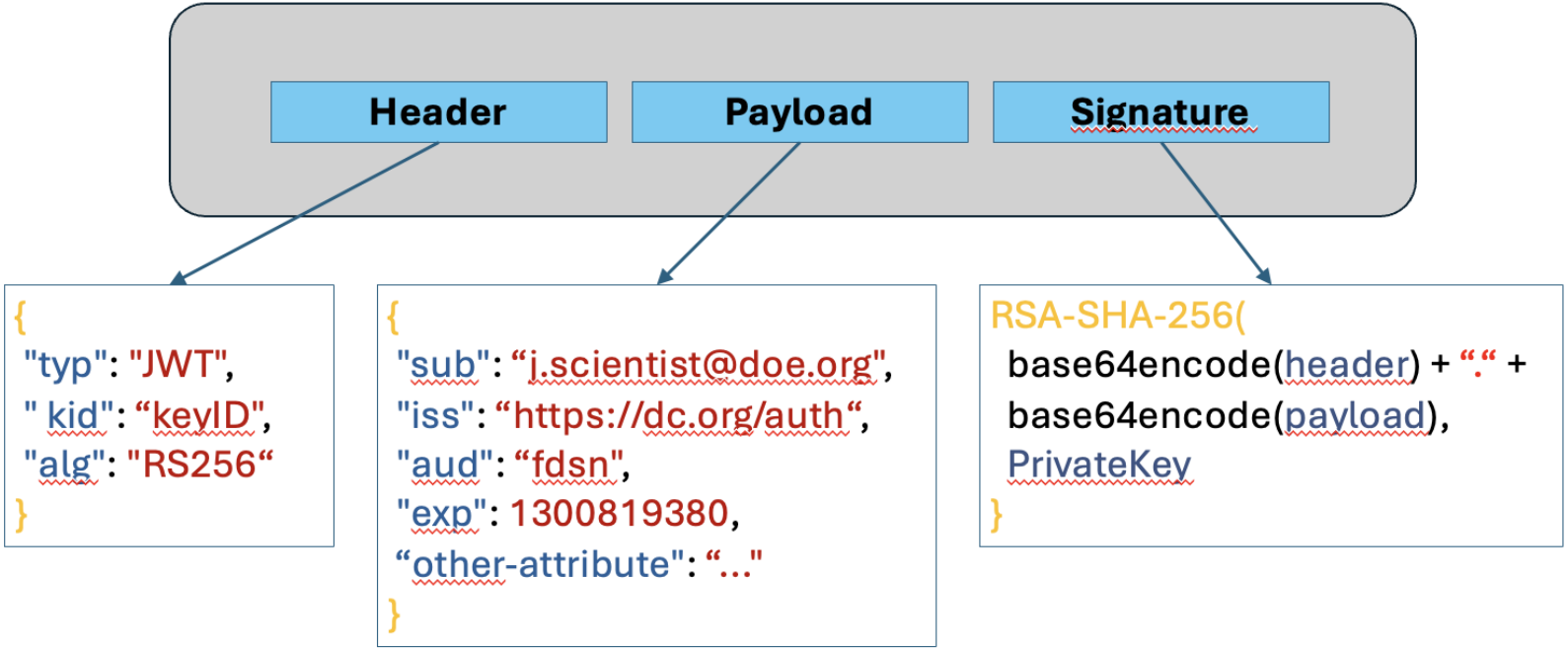


Get a token easily

- Command line tool to get a token.
- First time you log in through a web page at your home institution.
- After that, programatically with a Refresh Token.
- You will receive the token as soon as you authenticate.
- This needs to be securely stored.


```
{
  "access_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IkVBUy0yMDI
ImF1ZCI6ImZkc24iLCJpYXQiOjE3NTE1MzM1MDYsImV4cCI6MTc1MTUzNz
SAw4xIovtwmxfWjsgUM1NMDM1xfGMsyNYkuyigs-LnT_a11iEYkY5csg5r
lGDI5l6hydWSm8DnzcEilUNru3aB8O7_RmsLDqPcU8ltj-37uxhzH3kNJ-
AFHFD8TovQUTcSv5l_HYJNQV1tkZ40yMquRHp8WEKbtXwPzuW-HFtEi_Go
3xoqttpxl0UIVOeRnPB0VUKhHxJdNvI",
  "refresh_token": "5txf4mAjWbAxKyKjMRh88re3w4Mcg_oCoK4vxp
  "scope": "openid email profile eduperson_unique_id edupe
  "id_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IkVBUy0yMDI1Iiw
ZCI6ImVhcyIsImV4cCI6MTc1MTUzNzUwNiwiaWF0IjoxNzUxNTMzNTA2fQ
TUg6_U5ao-6rgzfcNoTZrWVuZsCgywpM9sz5Z1KLOpaJ36DoJ8bVU9Z13C
wRbjI4auHJb0xRj91fNG2k1H6Q5tsjkbCotDYpo9Yi_aFJtXOu5_T03GxQ
mgYCYmOJb_JSfgwN9fjm3c4qD3aKGNoToocdLFxycbNLAEkrkE9kNFopGw
  "token_type": "Bearer",
  "expires_in": 4000
}
```

JSON Web Token (JWT)



A real JSON Web Token

JWT Debugger

Debugger | Introduction | Libraries | Ask

JSON WEB TOKEN (JWT) COPY CLEAR

Valid JWT

Fix public key input errors to verify signature.


```
eyJhbGciOiJSUzI1NiIsImtpZCI6IkVBUy0yMDI1IiwidHlwIjoiSldUIn0.eyJz
dWIiOiI1MTliZDdiYy1iZTEyLTQ0OTMtYTcyNi03MmU3OTA2YjM0NDMiLCJpc3Mi
OiJodHRwczovL2dlb2Zvbi5nZnouZGUvZWFzMiIsImF1ZCI6ImZkc24iLCJpYXQi
OjE3NTE1MzM1MDYsImV4cCI6MTc1MTUzNzUwNiwiZW1haWwiOiJqYXZpZXJAZ2Z6
LmRlIn0.fkVwVKOHkj78wEZzVOq9bpWlAu-
KJiVsN9Kvpk0bP1iSb_dofv5r1Vnw9_k1ltRWK4fkf3dNs51_d_46lkFO5zczcq1
SAw4xIovtwmxfWjsgUM1NMDM1xfGMsyNYkuyigs-
LnT_a11iEYkY5csg5ruDRN9GMsP-kULiW8-
Vcqg8ox8m1po_fKfJzc6qx2lUd_Knf4GZ2meq2Ndagdwj5KI9AYPGunx5RQbrtOO
hR8YmlFFLefHX-tQ-
ORqF1p881zj9W8O1QRQw0X9ALkd41cUlGDI5l6hydWSm8DnzcEilUNru3aB8O7_R
msLDqPcU8ltj-37uxhzH3kNJ-
IB4syXmDf0iCp5QyCwPk_I22LS5QH1pAnhhJe4OU_LMN5TAYNaO-
3HjyxOExphBe6McWCzzd92zJV6UgDLLB-WTbHyx5C-
Nd3nSUxGszZJJxrCL3wnTFiAoOs6jAf8tfMAFHFD8TovQUTcSv5l_HYJNQV1tkZ4
0yMquRHp8WEKbtXwPzuW-
HFtEi_Gouv1W3Q7tgJgX5a93XOEgFa5N0BQv5iEX4Au2DUjAurBATlqEhxQabanh
y_JrbxM65U6Tx65dPqP_Js4zX6GiMBFQk5sfjMaqWLFeXm2tmIJ043XG5b6PSjka
```


JSON | CLAIMS TABLE COPY


```
{
  "alg": "RS256",
  "kid": "EAS-2025",
  "typ": "JWT"
}
```


DECODED PAYLOAD

JSON | CLAIMS TABLE COPY


```
{
  "sub": "519bd7bc-be12-4493-a726-72e7906b3443",
  "iss": "https://geofon.gfz.de/eas2",
  "aud": "fdsn",
  "iat": 1751533506,
  "exp": 1751537506,
  "email": "javier@gfz.de"
}
```

How to use it?

- Attach your Access Token in the header of your request. That‘s it!

```
Authorization: Bearer eyJhbGc[...]UIn0.eyJzd[...]WIiOiI.fkVwVK...
```

Benefits of new approach

- OAuth2 and JSON Web Tokens (JWT) are de-facto standards for AuthN/AuthZ
- Decoupling between Id Provider (e.g. eduGain) and Resource Provider (FDSN WS)
- Same endpoints for anonymous and authenticated requests
- This approach can be implemented in **all web services**
- Data Centres can include more attributes in the token if they need them
- Access token is valid only for some hours (limited risk if token is compromised)
- Not mandatory for data centres to issue their own tokens
- Data Centres **can trust one or more Identity Providers and accept their tokens**
- Station metadata can be now restricted if needed! Important for experiments using fiber optic cables whose position should remain secret (e.g. some DAS experiments)

Improvements for the community – A roadmap?

- Adopt JWT as our standard format for tokens.
  - EarthScope has done it.
  - EIDA has developed it also and it‘s ready to be in production.
  - GFZ has included it into SeisComP (waiting for proposal approval).

- Minimum number of fields taking into account GDPR. Any data centre can always add more fields, if needed.

- Use the HTTP header to transmit a token to the query method, if needed.

```
Authorization: Bearer <token>
```

Improvements for the community – A roadmap?

- Get rid of the queryauth method. (Finally!)

- Provide a simple, minimalistic way to issue tokens for small data centres.
  - Small data centres do not have the capacity to manage complex IT solutions.
  - They can rely on other provider and just use it!

- No need for any type of exchange (keys, passwords) between data centres.

Conclusion

- We have a unique oportunity to make a step forward and simplify our data provision system.
  - Adapt **JWT** as standard and **allow federations of data centres**.
  - Simplify in **a unique „query“ method** to request data.
  - **All services** could support authentication to improve statistics and analysis.
  - **No more passwords** for our users.
- This, plus the addition of the FDSN Data Centre Registry, would allow the user to **detach completely from where the data is hosted** (a unique, global seismological data centre).