GNAP

IETF 113 Hackathon

Aaron Parecki and Justin Richer

What is GNAP?

- Delegation protocol (like OAuth)
- Built on lessons learned from many years of OAuth deployments
- Minimizes security exposures through front-channel
- Flexible data access request for APIs and subject information

What was our focus?

- Protect requests with HTTP Signatures
- Make requests for tokens
- User interaction at AS
- Get usable access tokens

What did we build?

- New code:
  - PHP CLI & Web Client
  - SPA Client (JavaScript)
- Significant Updates to:
  - Java Web Client
  - Java Authorization Server
- Leveraged existing libraries and standards
  - Especially for HTTP structured fields and crypto primitives
  - https://github.com/ietf-wg-gnap/general/wiki/Implementations-and-Libraries

What did we learn?

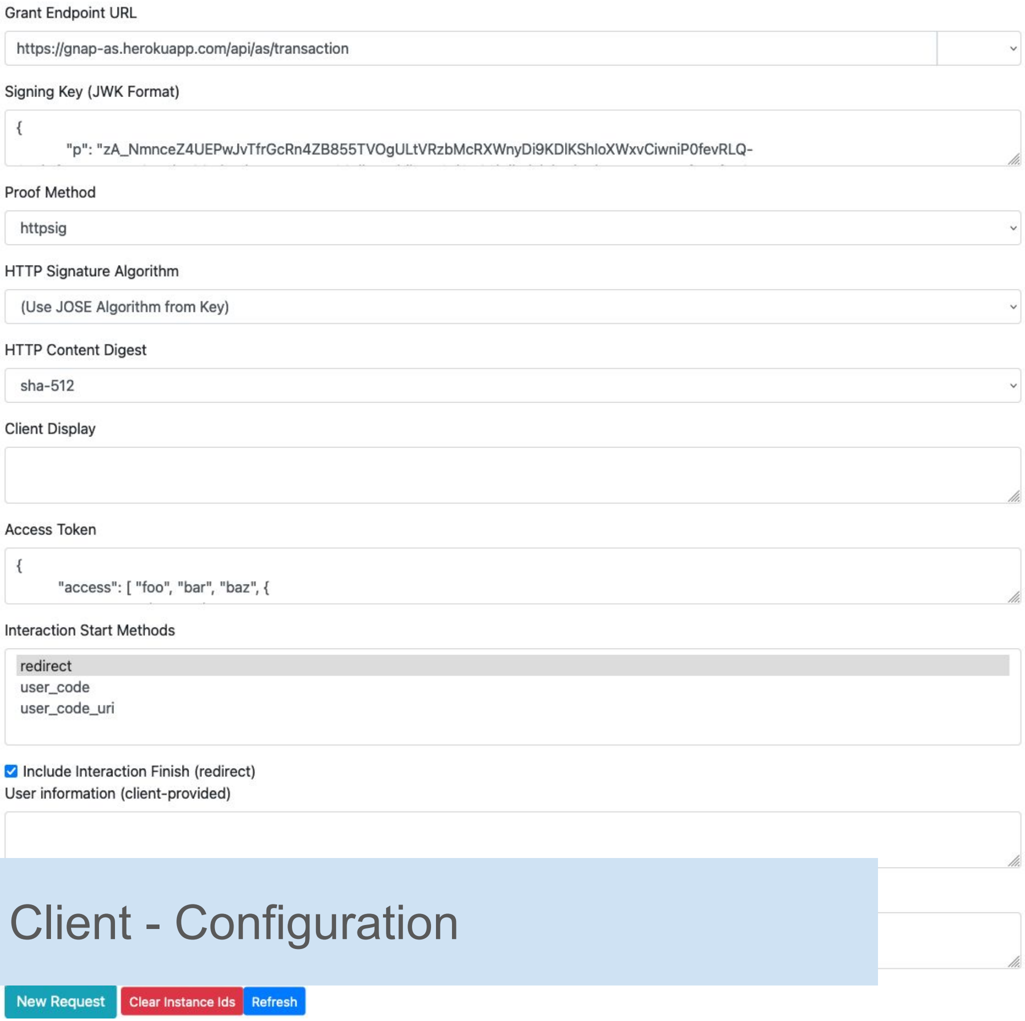
- HTTP Message Signatures is complex to do from scratch
  - Requires crypto, structured fields, HTTP message manipulation, etc.
  - Surprising fiddly bits (e.g., order of parameter fields)
  - Transparent if available within an HTTP library, but we aren’t there yet
- It’s actually possible to implement GNAP clients from scratch in relatively short order, if you already have a signing mechanism
- I still hate JavaScript

Improving the Specs

- GNAP
  - Need a way to communicate proof parameters (signature alg, digest alg, etc)
  - Polling uses an empty POST, why not GET?
  - Need to clarify grant lifecycle operations (already a set of open issues)
  - Need to reference hash methods from existing registry (open issue)
  - Need to clarify what the front-channel hash protects (probably with diagrams)
  - Some potential protocol cleanup/bikeshedding (“finish” vs “nonce”, “user_code.code”, etc)
- HTTP Structured Values
  - Would benefit from an implementer’s quickstart guide
- HTTP Message Signatures
  - Parameter order needs to be stable
  - Some library support, but more is needed (ours was all by hand)

Web-Based Java Client

Web-based Java Client - Configuration



Grant Endpoint URL

https://gnap-as.herokuapp.com/api/as/transaction

Signing Key (JWK Format)

```
{
        "p": "zA_NmnceZ4UEPwJvTfrGcRn4ZB855TVOgULtVRzbMcRXWnyDi9KDlKShloXWxvCiwniP0fevRLQ-
```

Proof Method

httpsig

HTTP Signature Algorithm

(Use JOSE Algorithm from Key)

HTTP Content Digest

sha-512

Client Display

Access Token

```
{
        "access": [ "foo", "bar", "baz", {
```

Interaction Start Methods

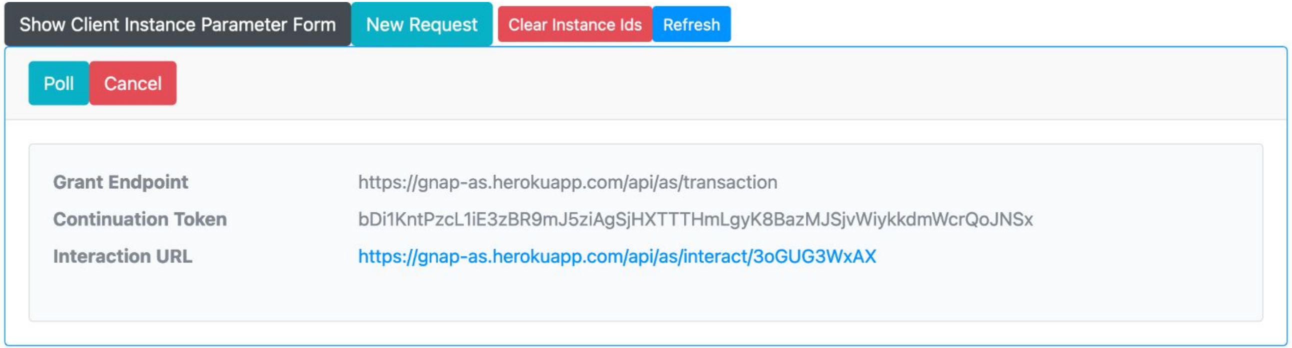
redirect

user_code

user_code_uri

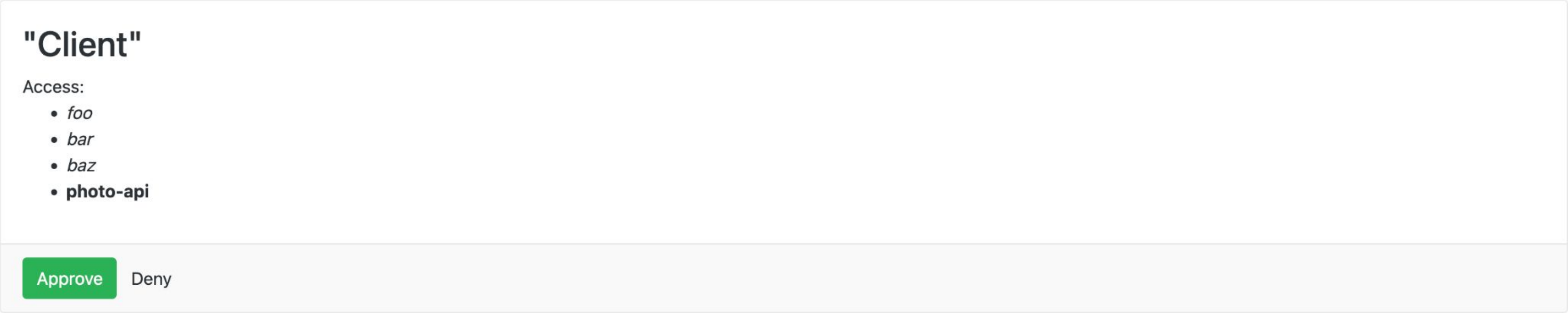
☑ Include Interaction Finish (redirect)

User information (client-provided)



Grant Endpoint	https://gnap-as.herokuapp.com/api/as/transaction
Continuation Token	bDi1KntPzcL1iE3zBR9mJ5ziAgSjHXTTTHmLgyK8BazMJSjvWiykkdmWcrQoJNSx
Interaction URL	https://gnap-as.herokuapp.com/api/as/interact/3oGUG3WxAX

Web-based Java Client - Grant Started

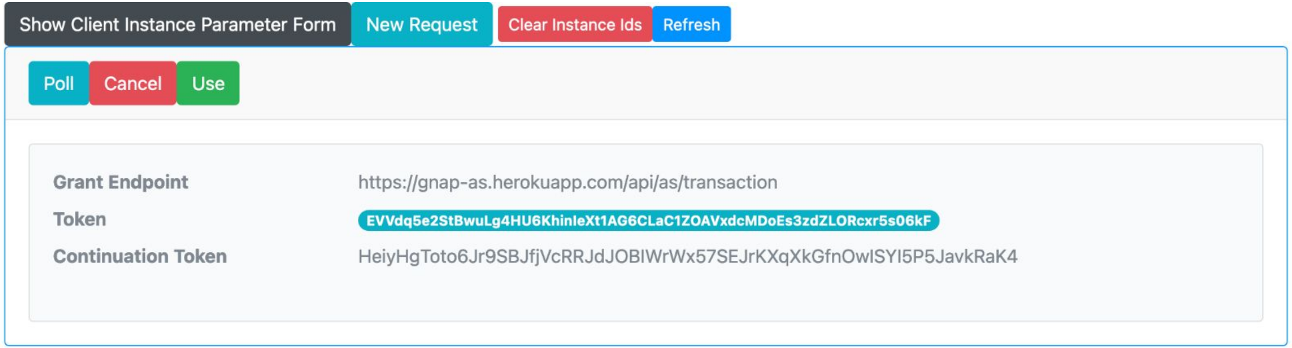


"Client"

Access:

- *foo*
- *bar*
- *baz*
- **photo-api**

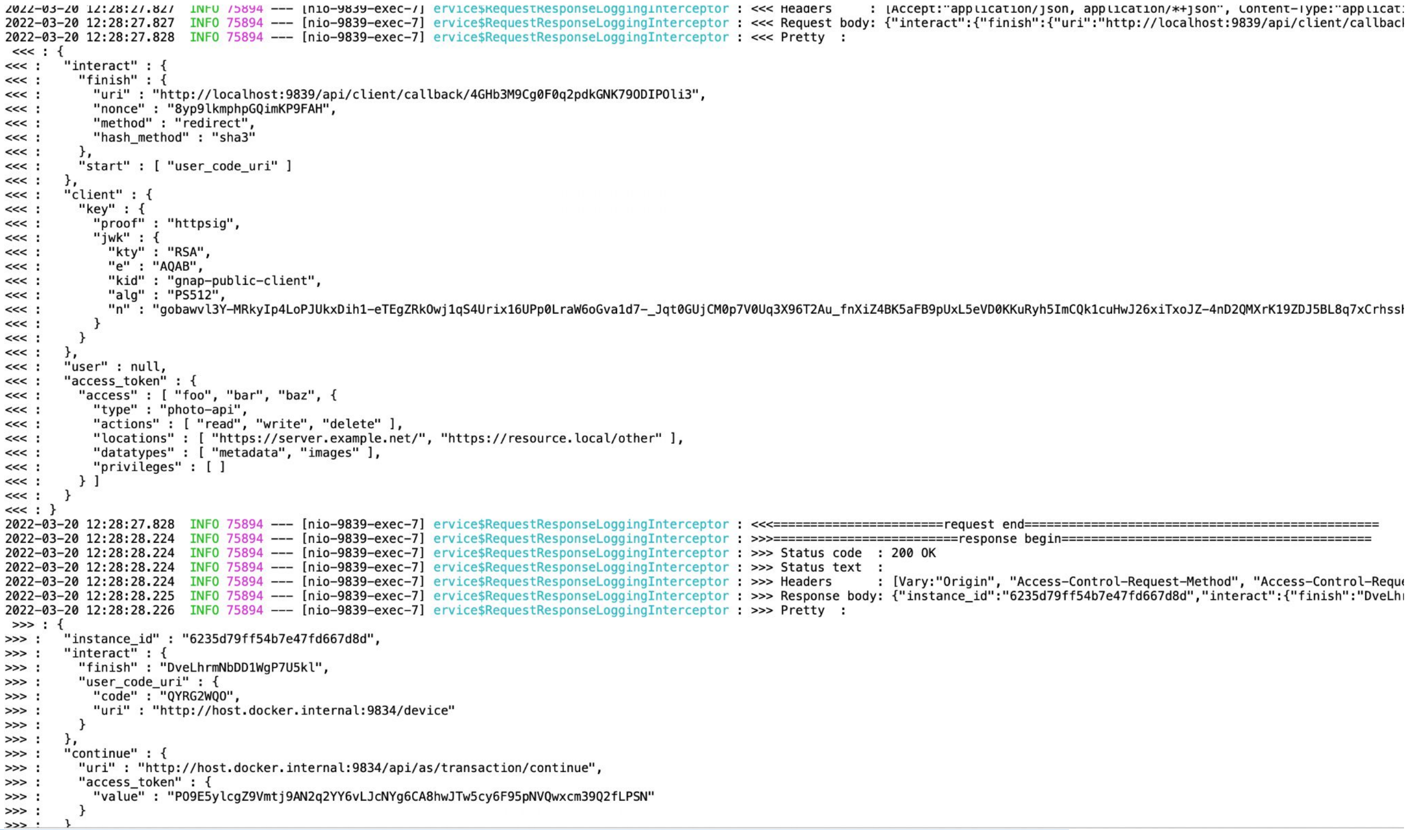
Web-based Java Client - Java AS Approval Page



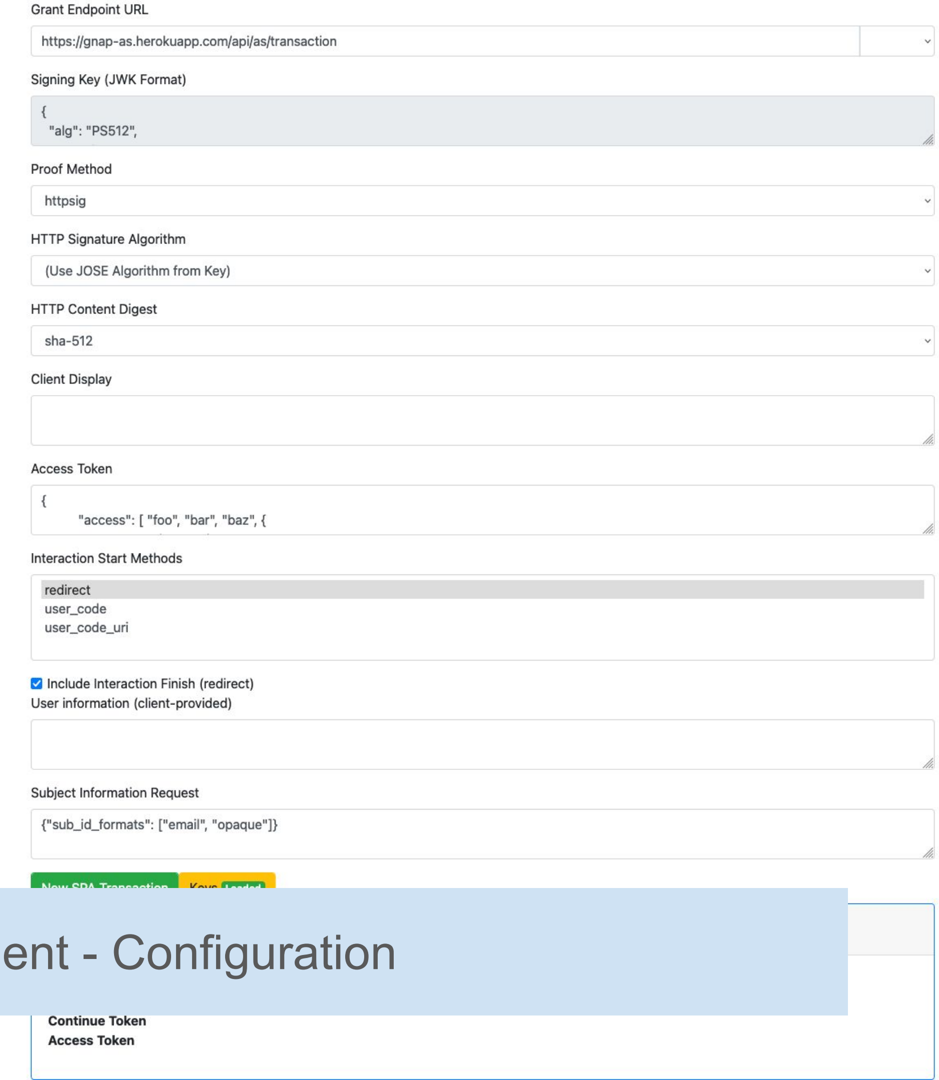
Grant Endpoint	https://gnap-as.herokuapp.com/api/as/transaction
Token	EVVdq5e2StBwuLg4HU6KhinleXt1AG6CLaC1ZOAVxdcMDoEs3zdZLORcxr5s06kF
Continuation Token	HeiyHgToto6Jr9SBJfjVcRRJdJOBIWrWx57SEJrKXqXkGfnOwISYI5P5JavkRaK4

Web-based Java Client - Grant Completed

Web-based Java Client - In the Background



```
2022-03-20 12:28:27.827  INFO 75894 --- [nio-9839-exec-7] ervice$RequestResponseLoggingInterceptor : <<< Headers     : [Accept:"application/json, application/*+json", Content-Type:"applicat
2022-03-20 12:28:27.827  INFO 75894 --- [nio-9839-exec-7] ervice$RequestResponseLoggingInterceptor : <<< Request body: {"interact":{"finish":{"uri":"http://localhost:9839/api/client/callbacl
2022-03-20 12:28:27.828  INFO 75894 --- [nio-9839-exec-7] ervice$RequestResponseLoggingInterceptor : <<< Pretty  :
 <<< : {
<<< :   "interact" : {
<<< :     "finish" : {
<<< :       "uri" : "http://localhost:9839/api/client/callback/4GHb3M9Cg0F0q2pdkGNK79ODIPOli3",
<<< :       "nonce" : "8yp9lkmphpGQimKP9FAH",
<<< :       "method" : "redirect",
<<< :       "hash_method" : "sha3"
<<< :     },
<<< :     "start" : [ "user_code_uri" ]
<<< :   },
<<< :   "client" : {
<<< :     "key" : {
<<< :       "proof" : "httpsig",
<<< :       "jwk" : {
<<< :         "kty" : "RSA",
<<< :         "e" : "AQAB",
<<< :         "kid" : "gnap-public-client",
<<< :         "alg" : "PS512",
<<< :         "n" : "gobawvl3Y-MRkyIp4LoPJUkxDih1-eTEgZRkOwj1qS4Urix16UPp0LraW6oGva1d7-_Jqt0GUjCM0p7V0Uq3X96T2Au_fnXiZ4BK5aFB9pUxL5eVD0KKuRyh5ImCQk1cuHwJ26xiTxoJZ-4nD2QMXrK19ZDJ5BL8q7xCrhssl
<<< :       }
<<< :     }
<<< :   },
<<< :   "user" : null,
<<< :   "access_token" : {
<<< :     "access" : [ "foo", "bar", "baz", {
<<< :       "type" : "photo-api",
<<< :       "actions" : [ "read", "write", "delete" ],
<<< :       "locations" : [ "https://server.example.net/", "https://resource.local/other" ],
<<< :       "datatypes" : [ "metadata", "images" ],
<<< :       "privileges" : [ ]
<<< :     } ]
<<< :   }
<<< : }
2022-03-20 12:28:27.828  INFO 75894 --- [nio-9839-exec-7] ervice$RequestResponseLoggingInterceptor : <<<=======================request end=================================================
2022-03-20 12:28:28.224  INFO 75894 --- [nio-9839-exec-7] ervice$RequestResponseLoggingInterceptor : >>>=========================response begin===========================================
2022-03-20 12:28:28.224  INFO 75894 --- [nio-9839-exec-7] ervice$RequestResponseLoggingInterceptor : >>> Status code  : 200 OK
2022-03-20 12:28:28.224  INFO 75894 --- [nio-9839-exec-7] ervice$RequestResponseLoggingInterceptor : >>> Status text  :
2022-03-20 12:28:28.224  INFO 75894 --- [nio-9839-exec-7] ervice$RequestResponseLoggingInterceptor : >>> Headers      : [Vary:"Origin", "Access-Control-Request-Method", "Access-Control-Reque
2022-03-20 12:28:28.225  INFO 75894 --- [nio-9839-exec-7] ervice$RequestResponseLoggingInterceptor : >>> Response body: {"instance_id":"6235d79ff54b7e47fd667d8d","interact":{"finish":"DveLhi
2022-03-20 12:28:28.226  INFO 75894 --- [nio-9839-exec-7] ervice$RequestResponseLoggingInterceptor : >>> Pretty  :
 >>> : {
>>> :   "instance_id" : "6235d79ff54b7e47fd667d8d",
>>> :   "interact" : {
>>> :     "finish" : "DveLhrmNbDD1WgP7U5kl",
>>> :     "user_code_uri" : {
>>> :       "code" : "QYRG2WQO",
>>> :       "uri" : "http://host.docker.internal:9834/device"
>>> :     }
>>> :   },
>>> :   "continue" : {
>>> :     "uri" : "http://host.docker.internal:9834/api/as/transaction/continue",
>>> :     "access_token" : {
>>> :       "value" : "PO9E5ylcgZ9Vmtj9AN2q2YY6vLJcNYg6CA8hwJTw5cy6F95pNVQwxcm39Q2fLPSN"
>>> :     }
>>> :   }
```



Grant Endpoint URL

https://gnap-as.herokuapp.com/api/as/transaction

Signing Key (JWK Format)

```
{
  "alg": "PS512",
```

Proof Method

httpsig

HTTP Signature Algorithm

(Use JOSE Algorithm from Key)

HTTP Content Digest

sha-512

Client Display

Access Token

```
{
        "access": [ "foo", "bar", "baz", {
```

Interaction Start Methods

redirect
user_code
user_code_uri

☑ Include Interaction Finish (redirect)

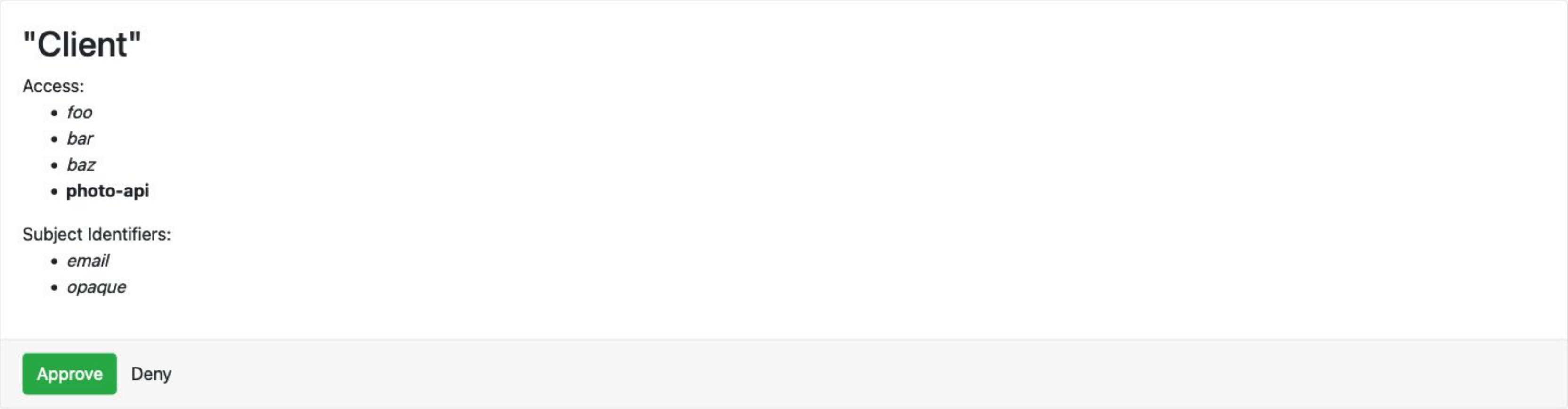
User information (client-provided)

Subject Information Request

```
{"sub_id_formats": ["email", "opaque"]}
```

Continue Token
Access Token

JavaScript SPA Client - Configuration



"Client"

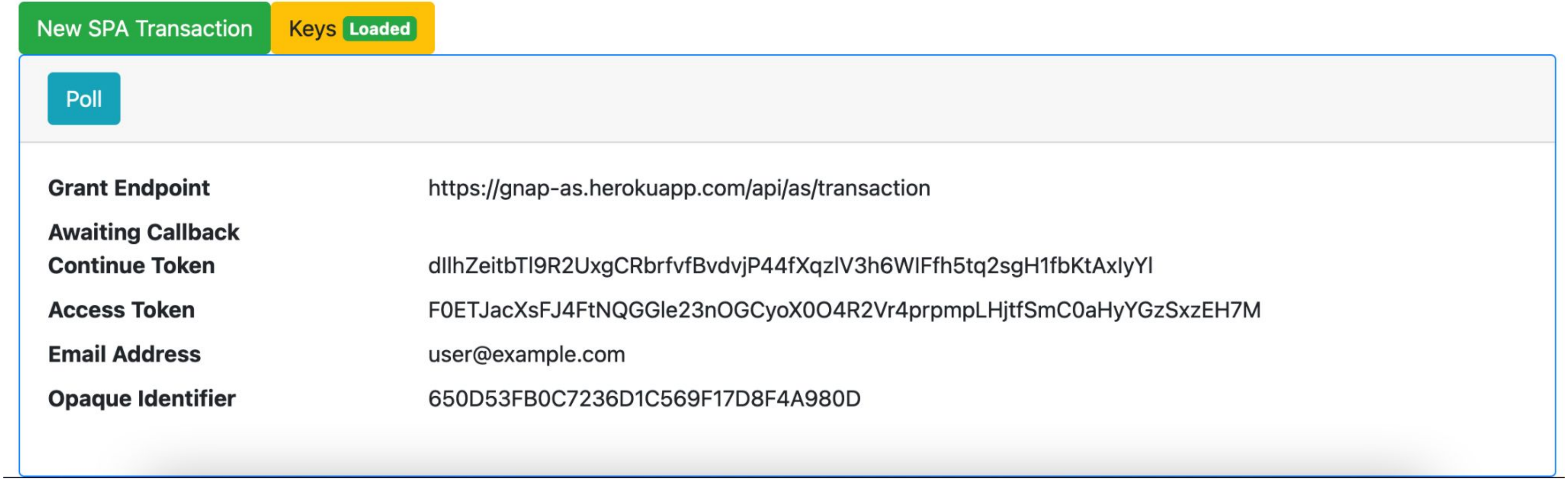
Access:

- *foo*
- *bar*
- *baz*
- **photo-api**

Subject Identifiers:

- *email*
- *opaque*

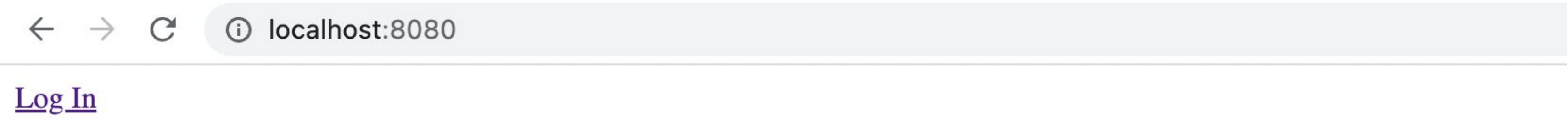
JavaScript SPA Client - Java AS Approval Page



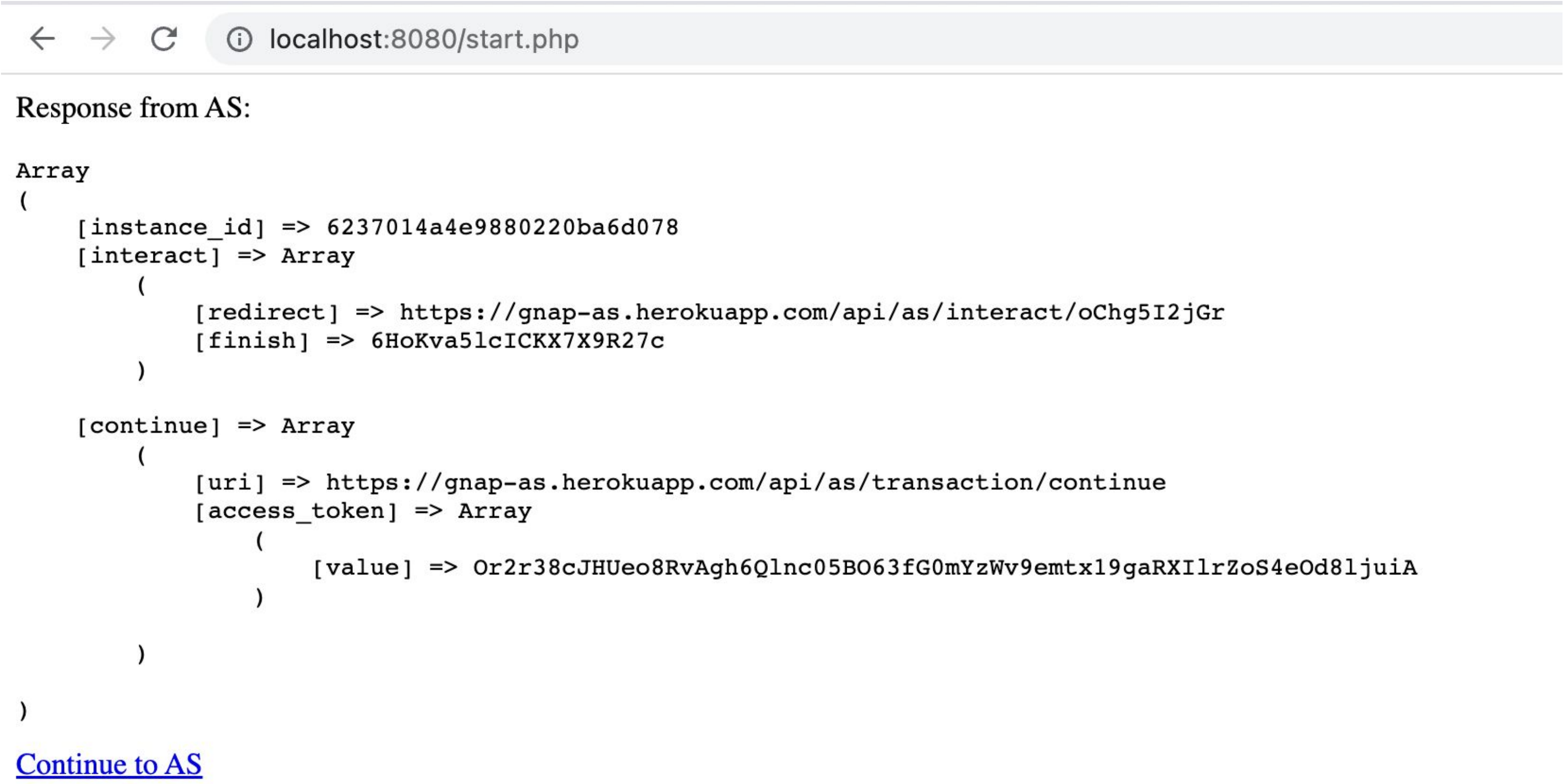
Grant Endpoint	https://gnap-as.herokuapp.com/api/as/transaction
Awaiting Callback	
Continue Token	dIlhZeitbTl9R2UxgCRbrfvfBvdvjP44fXqzlV3h6WIFfh5tq2sgH1fbKtAxIyYl
Access Token	F0ETJacXsFJ4FtNQGGle23nOGCyoX0O4R2Vr4prpmpLHjtfSmC0aHyYGzSxzEH7M
Email Address	user@example.com
Opaque Identifier	650D53FB0C7236D1C569F17D8F4A980D

JavaScript SPA Client - Results

Web-Based PHP Client



PHP Web Client - Start

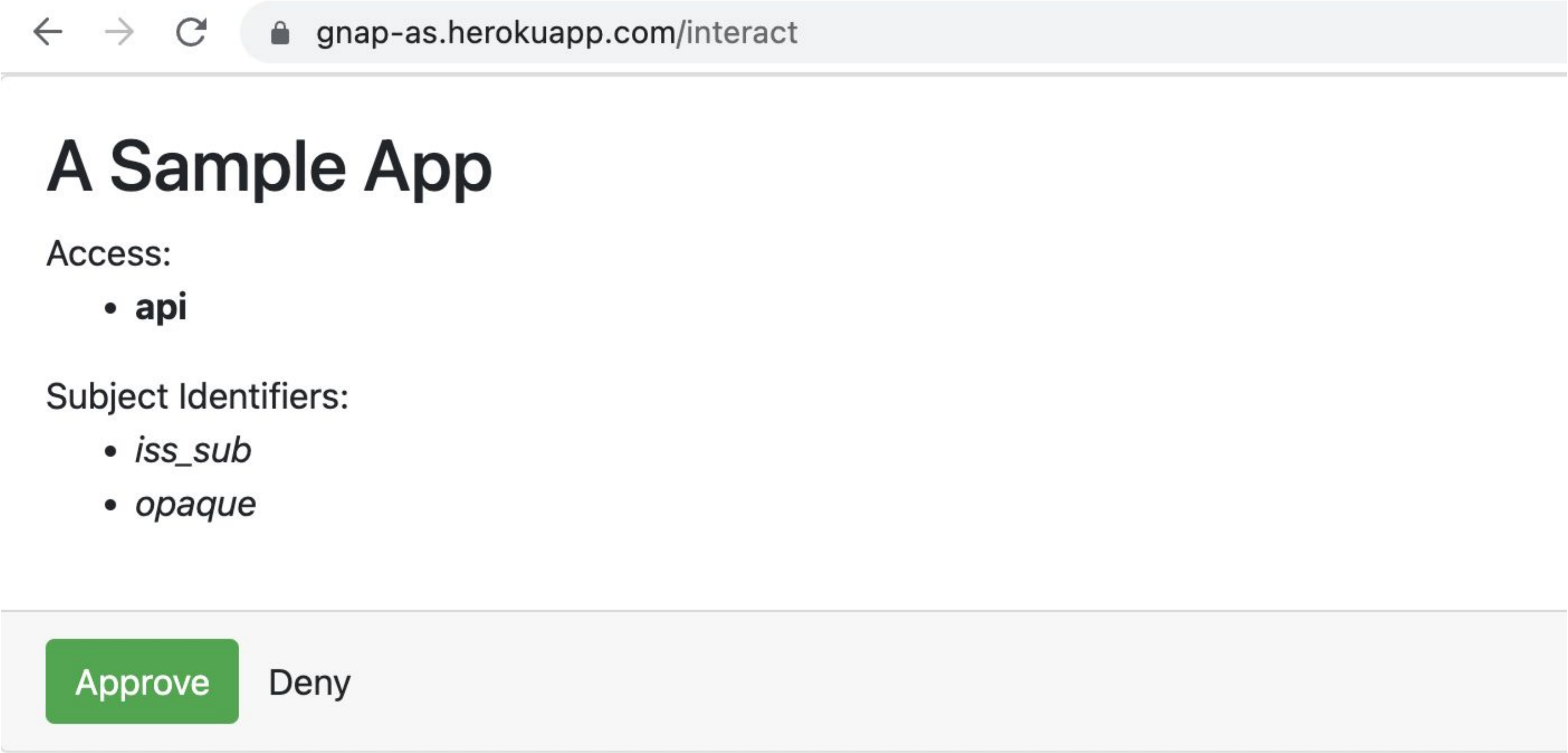


Response from AS:

```
Array
(
    [instance_id] => 6237014a4e9880220ba6d078
    [interact] => Array
        (
            [redirect] => https://gnap-as.herokuapp.com/api/as/interact/oChg5I2jGr
            [finish] => 6HoKva5lcICKX7X9R27c
        )

    [continue] => Array
        (
            [uri] => https://gnap-as.herokuapp.com/api/as/transaction/continue
            [access_token] => Array
                (
                    [value] => Or2r38cJHUeo8RvAgh6Qlnc05BO63fG0mYzWv9emtx19gaRXIlrZoS4eOd8ljuiA
                )

        )

)
```

Continue to AS

PHP Web Client - Processing Response



gnap-as.herokuapp.com/interact

A Sample App

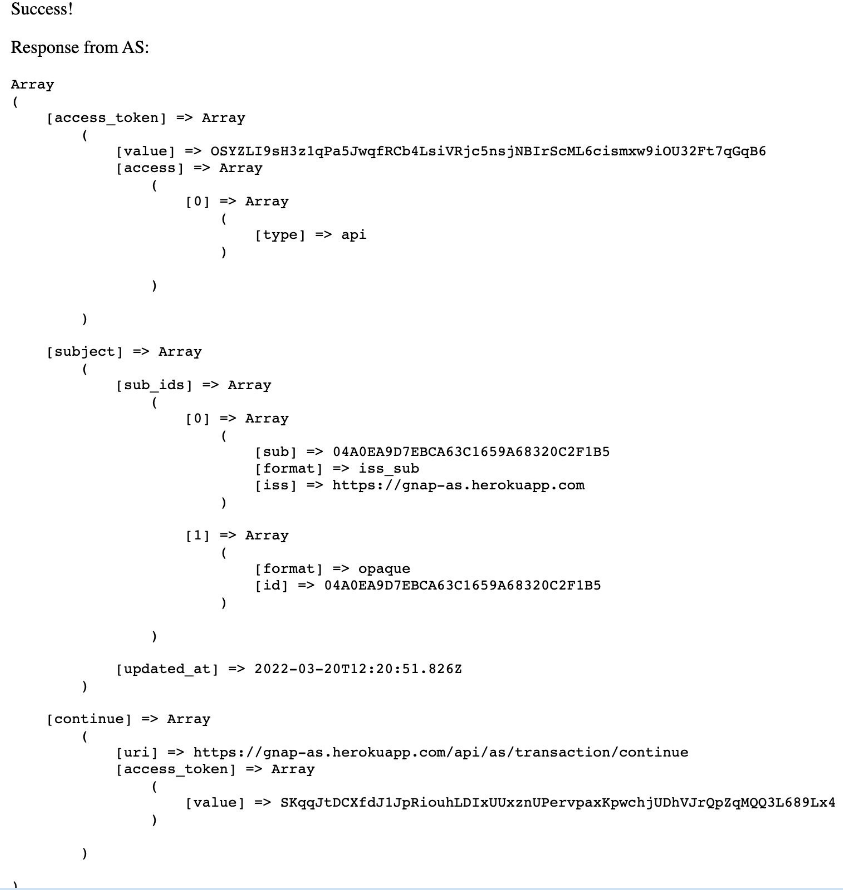
Access:

- **api**

Subject Identifiers:

- *iss_sub*
- *opaque*

PHP Web Client - Java AS Approval Page

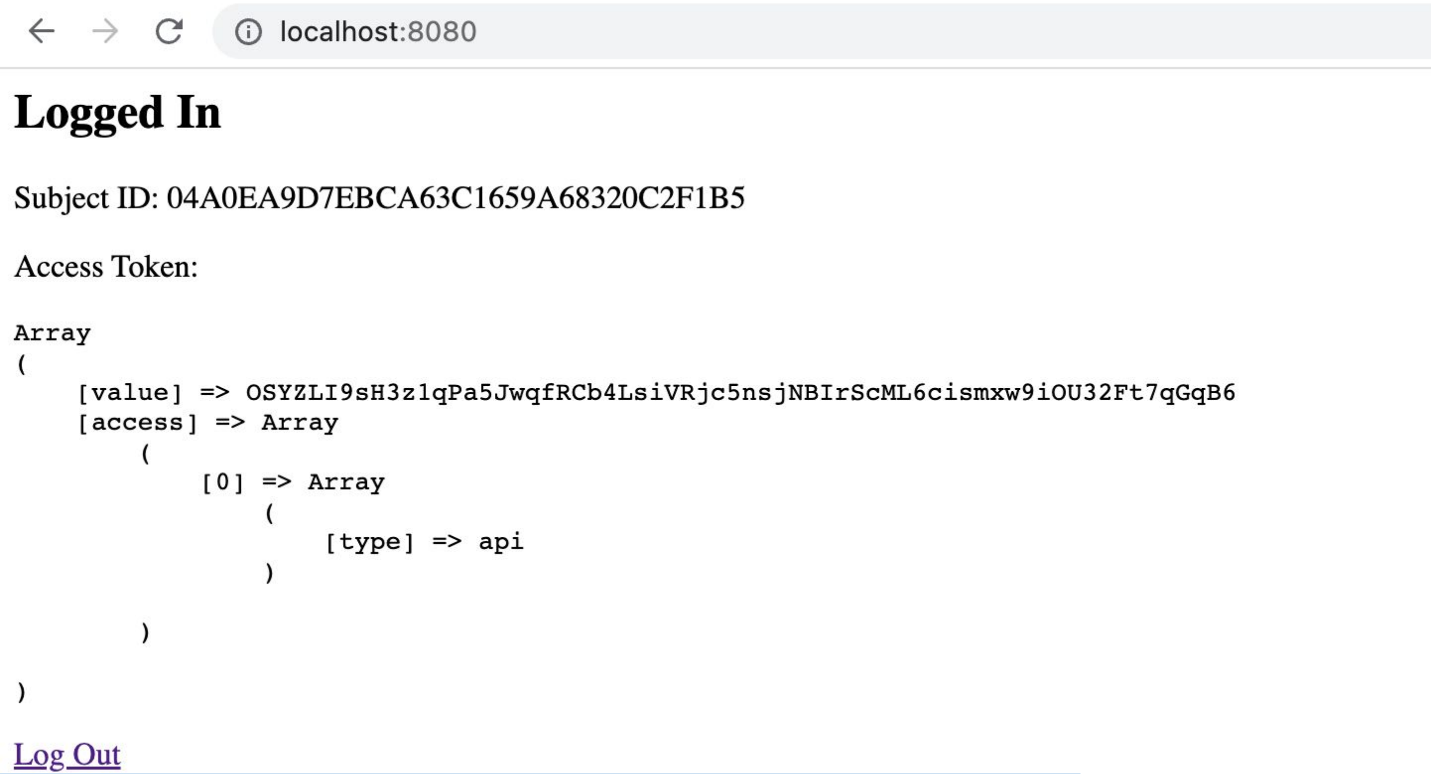


Success!

Response from AS:

```
Array
(
    [access_token] => Array
        (
            [value] => OSYZLI9sH3z1qPa5JwqfRCb4LsiVRjc5nsjNBIrScML6cismxw9iOU32Ft7qGqB6
            [access] => Array
                (
                    [0] => Array
                        (
                            [type] => api
                        )

                )

        )

    [subject] => Array
        (
            [sub_ids] => Array
                (
                    [0] => Array
                        (
                            [sub] => 04A0EA9D7EBCA63C1659A68320C2F1B5
                            [format] => iss_sub
                            [iss] => https://gnap-as.herokuapp.com
                        )

                    [1] => Array
                        (
                            [format] => opaque
                            [id] => 04A0EA9D7EBCA63C1659A68320C2F1B5
                        )

                )

            [updated_at] => 2022-03-20T12:20:51.826Z
        )

    [continue] => Array
        (
            [uri] => https://gnap-as.herokuapp.com/api/as/transaction/continue
            [access_token] => Array
                (
                    [value] => SKqqJtDCXfdJ1JpRiouhLDIxUUxznUPervpaxKpwchjUDhVJrQpZqMQQ3L689Lx4
                )

        )

)
```

PHP Web Client - Response from AS



Logged In

Subject ID: 04A0EA9D7EBCA63C1659A68320C2F1B5

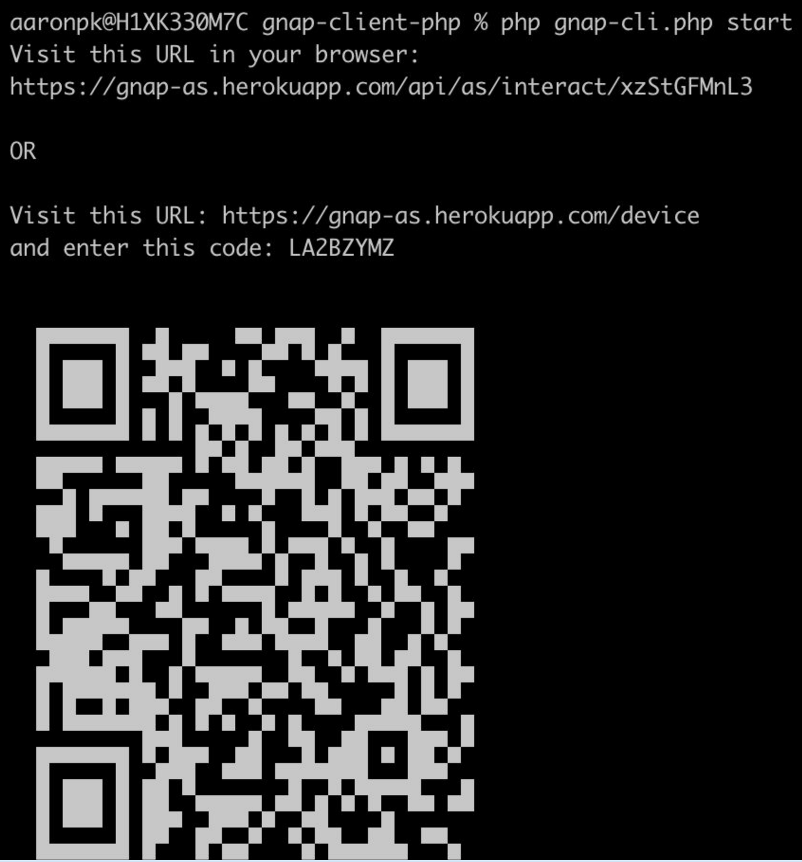
Access Token:

```
Array
(
    [value] => OSYZLI9sH3z1qPa5JwqfRCb4LsiVRjc5nsjNBIrScML6cismxw9iOU32Ft7qGqB6
    [access] => Array
        (
            [0] => Array
                (
                    [type] => api
                )

        )

)
```

Log Out

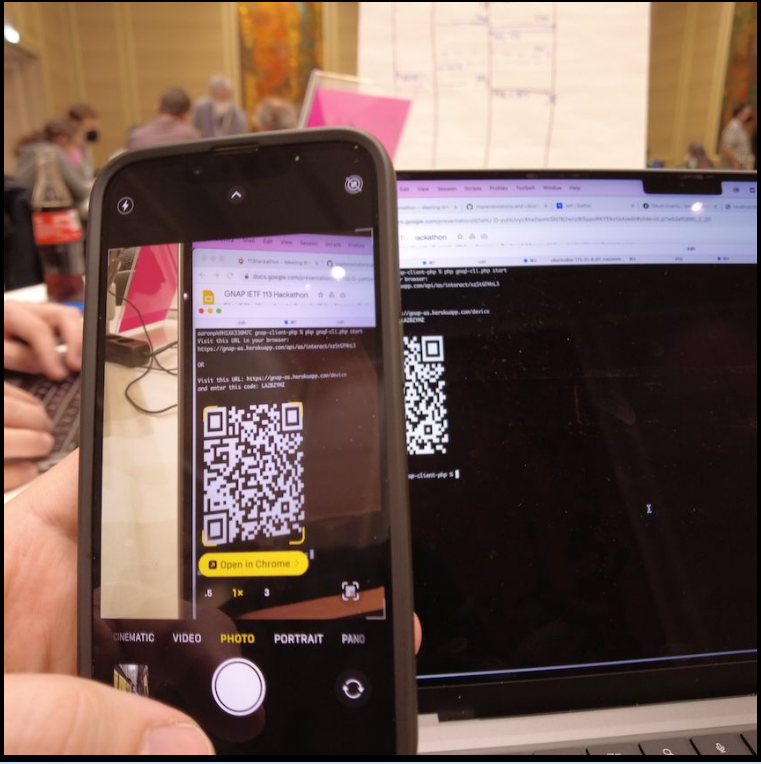
PHP Web Client - Logged In

Command Line PHP Client



```
aaronpk@H1XK330M7C gnap-client-php % php gnap-cli.php start
Visit this URL in your browser:
https://gnap-as.herokuapp.com/api/as/interact/xzStGFMnL3

OR

Visit this URL: https://gnap-as.herokuapp.com/device
and enter this code: LA2BZYMZ
```

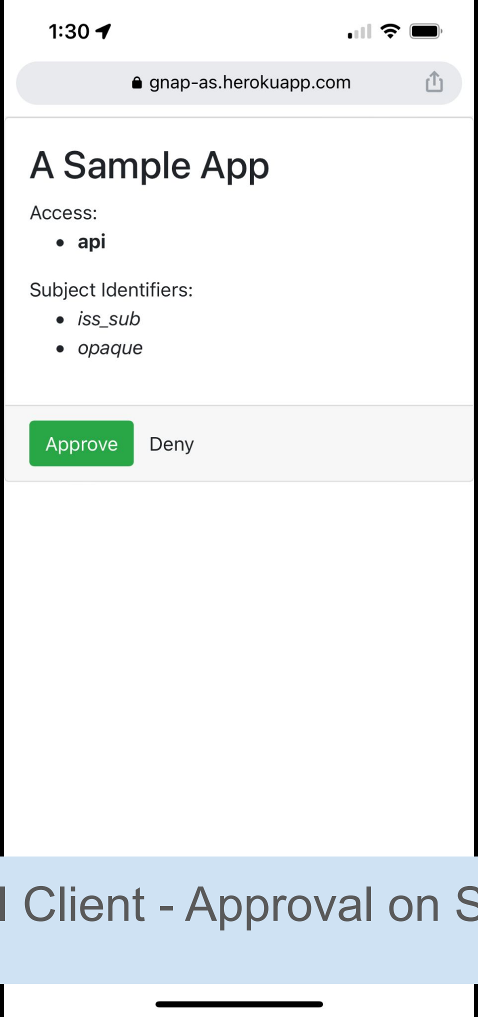
PHP CLI Client - Start



```
aaronpk@MX1XK330M7C gnap-client-php % php gnap-cli.php start
Visit this URL in your browser:
https://gnap-as.herokuapp.com/api/as/interact/xz5tGfNeL3

OR

Visit this URL: https://gnap-as.herokuapp.com/device
and enter this code: LAZBZYNZ
```

PHP CLI Client - Scanning QR Code

PHP CLI Client - Approval on Second Device



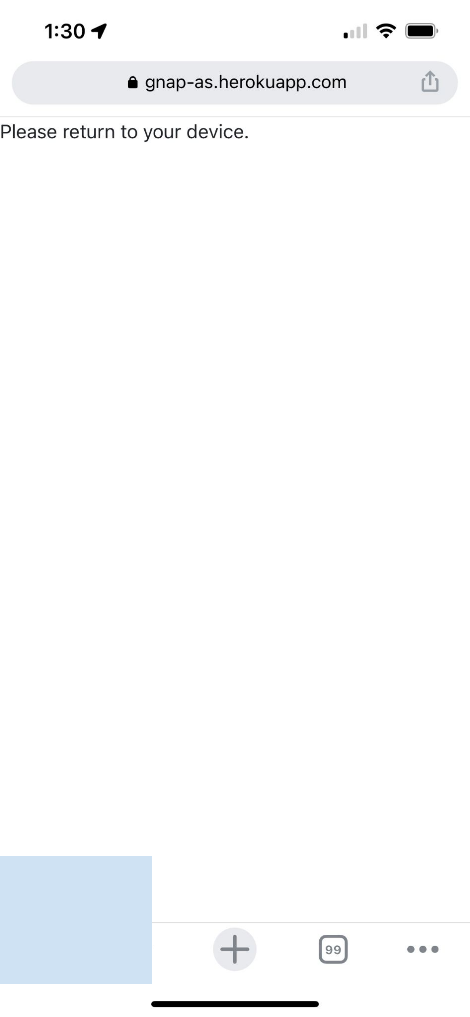
A Sample App

Access:

- **api**

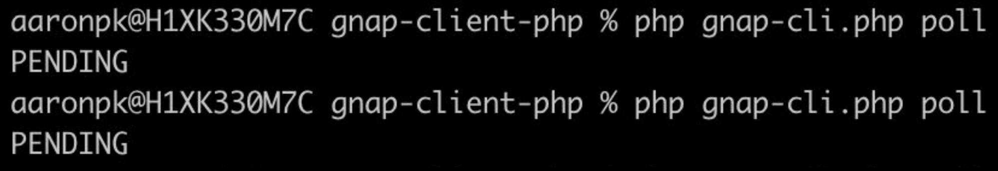
Subject Identifiers:

- *iss_sub*
- *opaque*

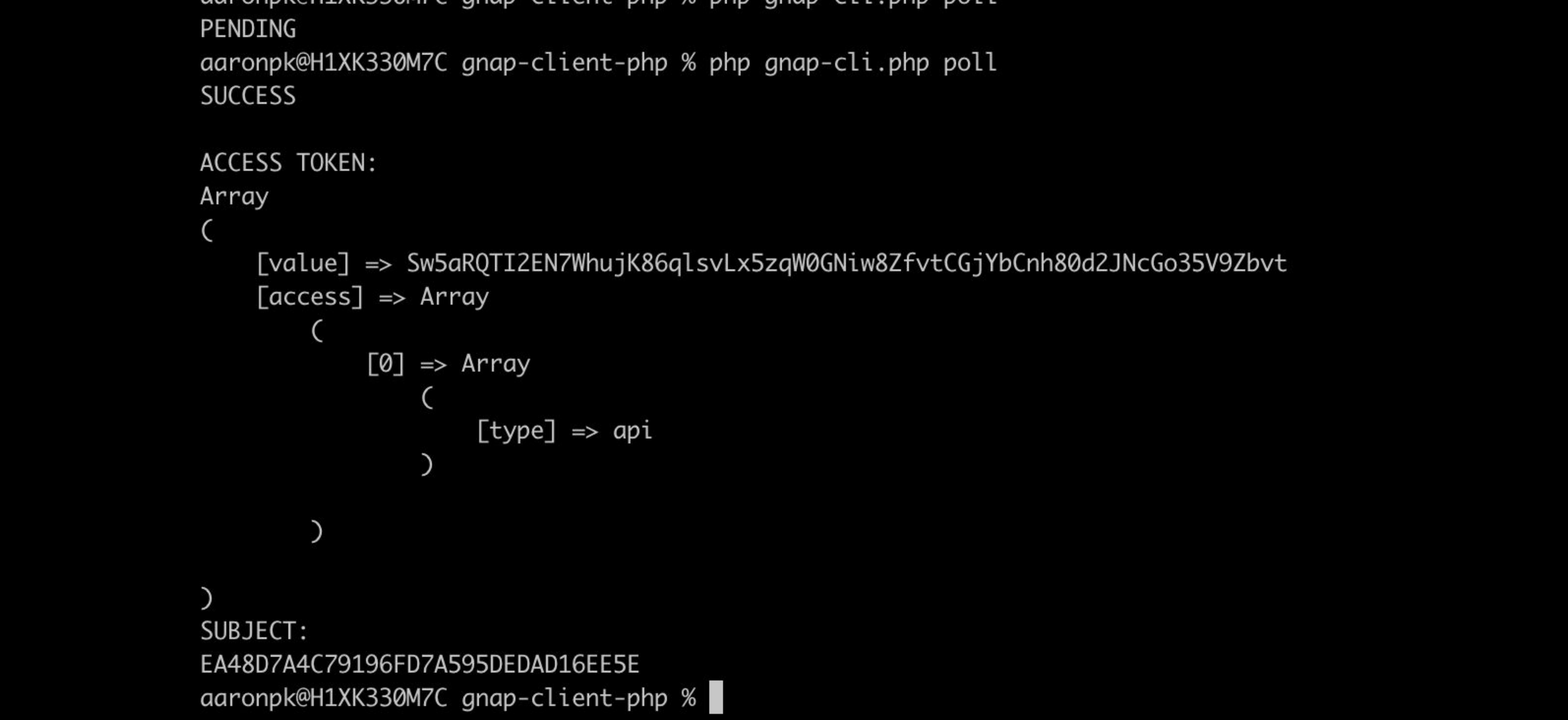


Please return to your device.

PHP CLI Client - Polling



```
aaronpk@H1XK330M7C gnap-client-php % php gnap-cli.php poll
PENDING
aaronpk@H1XK330M7C gnap-client-php % php gnap-cli.php poll
PENDING
```



```
aaronpk@H1XK330M7C gnap-client-php % php gnap-cli.php poll
PENDING
aaronpk@H1XK330M7C gnap-client-php % php gnap-cli.php poll
SUCCESS

ACCESS TOKEN:
Array
(
    [value] => Sw5aRQTI2EN7WhujK86qlsvLx5zqW0GNiw8ZfvtCGjYbCnh80d2JNcGo35V9Zbvt
    [access] => Array
        (
            [0] => Array
                (
                    [type] => api
                )

        )

)
SUBJECT:
EA48D7A4C79196FD7A595DEDAD16EE5E
aaronpk@H1XK330M7C gnap-client-php %
```

PHP CLI Client - Results