Interweave Portal Context Launch

To enable launch of the Interweave Portal from a partner system with a selected patient in context the partner system must be able to satisfy one of the following:

1 JWT Assertion

Where a partner system does not have access to an Identity Provider as outlined in 2 - OICD/SAML Identity Provider, one of the following methods may be used:

1.1 JWT Assertion (POST)

Generate an HTTP POST Request with the following structure:

```
POST /code/provider/<providerid> HTTP/1.1
Host: <tenant>.portal.<environment>.<region>.nhs.uk
Content-Type: application/x-www-form-urlencoded
Content-Length: 618

assertion=eyJhbGciOiJSUzUxMiIsInR5cCI6IkpXVCJ9.eyJqdGkiOiI8anRpPiIsIml
hdCI6IjxpYXQ-
IiwiZXhwIjoiPGV4cD4iLCJwYXQiOnsibmhzIjoiPG5ocz4iLCJmYW0iOiI8ZmFtPiIsIm
dpdiI6IjxnaXY-IiwiZG9iIjoiPGRvYj4ifSwidXNyIjp7InN1YiI6IjxzdWI-
IiwiZmFtIjoiPGZhbT4iLCJnaXYiOiI8Z2l2PiIsInJvbCI6Ijxyb2w-
In19.VjB0eAuxgUgvL_52OYnEJ70vZzlt1KpwhqDSANyU71xd0u9Dcf-
u0QzPjyUbMry2Odu69f3LKLyDrcaQWWIm3QqZqy0O5sJtUtAhmFgQ5f9Q9Q7adxyhD0A0l
sw1h6_QKdv7EE-
LIglnmShSNNCEzS7yY5BYCo6eCGKTnDWkk8g2ZDbj8YptFScQ0jXaDVpb3uwgP_NN33Khq
W50SW-V0vXvYzFKiKY4b_xfSs7N34cUyMgb4ndQ-
JKo6CxHODepWmD0KJT03z6xjzxFsaf91yNDoN37l2pPLz3uVjVpSGLv6RegoBSiUl4eFBT
_kqH4TP8IIjacKHp-IKte3T5izQ
```

Where the assertion parameter is a signed json web token with the following payload structure:

```
{
  "jti": "<jti>",
  "iat": "<iat>",
  "exp": "<exp>",
  "pat": {
    "nhs": "<nhs>",
    "fam": "<fam>",
    "giv": "<giv>",
    "dob": "<dob>"
  },
  "usr": {
    "sub": "<sub>",
    "fam": "<fam>",
    "giv": "<giv>",
    "rol": "<rol>"
  }
}
```

Here:

- jti is a JWT ID and must be unique per context launch
- iat and exp are is the issue time and expiry time of the launch token in seconds
- pat object is the details of the patient to be context launched, and conforms to the same rules as outlined in the OIDC/SAML Identity Provider section.
- usr object represents information about the user initiating the context launch
    - sub is the unique id of the user in the partner system
    - fam is the family name of the user
    - giv is the given name of the user
    - rol is the role of the user in the partner system

The usr.sub, usr.fam and usr.giv properties are required, the usr.rol parameter is only required if the partner system wishes the launching user to be assigned a non-default role within the Interweave Portal.
The public key and algorithm used to sign the JWT must be provided before this login system can be configured.
A successful assertion request will generate an HTTP response with an opaque code:

```
HTTP/1.1 200 Ok

{ "code": "<code>" }
```

With the code received generate an HTTP Request with the following structure within a browser:

```
GET /Login/Provider/<providerid>?jwt=<jwt> HTTP/1.1
Host: <tenant>.portal.<environment>.<region>.nhs.uk
```

Where the jwt is a signed json web token with the following structure:

```
{
  "code": "<code>"
}
```

The code parameter is the opaque code returned from the initial POST request. The same signing key should be used for the assertion and code exchange.

This method is preferred over the HTTP GET method below as the user and patient details do not need to be passed in the request query where they may potentially be saved in browser history and/or request logs.

1.2 JWT Assertion (GET)

Generate an HTTP GET Request with the following structure within a browser:

```
GET /Login/Provider/<providerid>?jwt=<jwt> HTTP/1.1
Host: <tenant>.portal.<environment>.<region>.nhs.uk
```

Where jwt is a signed json web token with the same structure as set out in the HTTP POST section above.

The public key and algorithm used to sign the JWT must be provided before this login system can be configured.

2 OIDC/SAML Identity Provider

Where the partner system has access to an internet facing OIDC or SAML Identity Provider (e.g. Azure AD) be able to generate a url of the following structure:

```
https://portal.<environment>.<region>.nhs.uk/Login/Provider/<providerid>?pat.nhs=<nhsnumber>&pat.fam=<familyname>&pat.giv=<givenname>&pat.dob=<dateofbirth>
```

Where environment is the specific Interweave Portal environment to launch, providerid is a unique id for the login system which will be provided on setup, and pat.nhs, pat.giv, pat.fam and pat.dob are query string parameters containing the patient's NHS number, given name, family name and date of birth respectively. At a minimum the pat.nhs paramter must be present to context launch a patient. The relevant OIDC/SAML keys, urls and certificates must be exchanged between the Interweave Portal and the partner system before this login system can be configured.