|  |  |  |  |
| --- | --- | --- | --- |
| Document filename: | **NHS login Interface Specification – Provision Account** | | |
| Directorate / Programme | **NHS login Programme** |  |  |
| Document Reference | **CID-IS-P** | Status | **DRAFT** |
| Information Asset Owner | Melissa Ruscoe | Version | **V1.0** |
| Author | Priyanka Mittal | Version issue date | **31 Jan. 24** |

**NHS login**

**Interface Specification – Provision Account**

**Document Management**

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Summary of Changes** |
| V1.0 Draft | 31-Jan-24 | First draft version available |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Reviewers**

This document must be reviewed by the following people:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reviewer name** | **Title / Responsibility** | **Date** | **Version** |
| Melissa Ruscoe | Programme Director | 31-Jan-24 | V1.0 |
| Matthew Brown | Lead Solution Architect | 31-Jan-24 | V1.0 |
| Priyanka Mittal | Senior Solution Architect | 31-Jan-24 | V1.0 |
| Sam Payne | Cyber Security Consultant | 31-Jan-24 | V1.0 |

**Approved by**

This document must be approved by the following people:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Title / Responsibility** | **Date** | **Version** |
| Melissa Ruscoe | Programme Director | 31-Jan-24 | V1.0 |
| Hayden Gillmore | Product Owner | 31-Jan-24 | V1.0 |

**Document Control:**

The controlled copy of this document is maintained in the NHS England corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

[1 Introduction 4](#_Toc157521813)

[1.1 Purpose of Document 4](#_Toc157521814)

[1.2 Audience 4](#_Toc157521815)

[1.3 Definitions 4](#_Toc157521816)

[2 Specification Status 5](#_Toc157521817)

[2.1 Scope / Constraints 5](#_Toc157521818)

[2.2 Changes in this version 5](#_Toc157521819)

[3 Information Flows 6](#_Toc157521820)

[3.1 Overview 6](#_Toc157521821)

[3.2 Token Endpoint 7](#_Toc157521822)

[3.2.1 Token Request 7](#_Toc157521823)

[3.2.2 Token Request Validation 8](#_Toc157521824)

[3.2.3 Token Response 8](#_Toc157521825)

[3.3 Provision Account Endpoint 10](#_Toc157521826)

[3.3.1 Provision Account Request 11](#_Toc157521827)

[3.3.2 Provision Account Success Response 12](#_Toc157521828)

[3.3.3 Provision Account Error Response 12](#_Toc157521829)

[4 Tokens 14](#_Toc157521830)

[4.1 JWT for Client Authorization 14](#_Toc157521831)

[4.1.1 Token Header 14](#_Toc157521832)

[4.1.2 Token Payload 14](#_Toc157521833)

[4.1.3 JWT Signature 15](#_Toc157521834)

[4.2 Access Token Payload 15](#_Toc157521835)

[4.3 JWT Signing 15](#_Toc157521836)

[5 References 16](#_Toc157521837)

# Introduction

Purpose of Document

The NHS England NHS login Platform implements a Service Provider role to create the identity of an End-User by enabling a Service Consumer to send basic profile information about the End-User in an interoperable manner.

This document defines the provision account interface implemented by the NHS England NHS login Platform and describes the data flow supported by this interface.

Audience

The primary audiences for this document are:

* NHS login Programme team
* NHS England – Platform Delivery Team
* NHS England – Other Delivery teams
* 3rd Party GP system suppliers and/or other approved system suppliers integrating with the NHS England NHS login Platform

Definitions

Where used in this document set, the keywords MUST, SHOULD and MAY are to be interpreted as follows:

* **MUST**: This word, or the terms “**REQUIRED**” or “**SHALL**”, means that the definition is an absolute` requirement of the specification.
* **SHOULD**: This word, or the adjective “**RECOMMENDED**”, means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications **MUST** be understood and carefully weighed before choosing a different course.
* **MAY**: This word, or the adjective “**OPTIONAL**”, means that an item is truly optional. One implementer may choose to include the item because a particular implementation requires it or because the implementer feels that it enhances the implementation while another implementer may omit the same item. An implementation which does not include a particular option **MUST** be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option **MUST** be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides).

# Specification Status

Scope / Constraints

* HTTP is not supported – all HTTP-based flows must be HTTPs (using TLS v1.2 or above)
* All examples contained within this document are non-normative.

Changes in this version

Version 1.0 of this specification is the first version which can be shared externally.

# Information Flows

This section describes how the NHS login Platform supports information flows relating to Provision Account.

Overview

Broadly the pattern is:

1. Service Consumer provides its credentials to the NHS login Platform
2. NHS login Platform authenticates the Service Consumer and authorizes access to the Provision Account endpoint
3. Service Consumer accesses the Provision Account endpoint with a single message, within the time constraint of the provided access token

The Service Consumer is authenticated and is authorized to the NHS login platform using a standard OAuth Client Authorization Grant Flow – in this flow the Service Consumer is the OAuth Client.

A diagram of a service

Description automatically generated

1. The Service Consumer prepares and signs a JWT to get authenticated and authorized by the NHS login platform
2. The Service Consumer sends the request to the NHS login Platform token endpoint directly via HTTPs
3. The NHS login Platform validates the Authorization Request
4. The NHS login Platform authenticates the Service Consumer by validating the JWT signature
5. The NHS login Platform Authorizes the Service Consumer
6. The Service Consumer receives a response that contains an Access Token in the response body
7. The Service Consumer adds the bearer token to the Authorization header and sends a provision request with user data in the body to NHS login Platform.
8. The NHS login Platform checks eligibility of the supplied data and returns the appropriate response back to the Service Consumer.
9. The Service Consumer can use the Access Token multiple times while TTL (300 seconds) is valid.

Token Endpoint

### Token Request

References:

* RFC7523 - JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants [1]

A Token request is used to obtain an Access Token. The Service Consumer (client) sends a Token Request to the Token Endpoint to obtain a Token Response.

The Client sends the parameters to the Token Endpoint using the HTTP POST method and the application/x-www-form-urlencoded serialization – the request must be sent using TLS v1.2 or above.

Table 1: Token Request Parameters

|  |  |  |
| --- | --- | --- |
| Parameter | Req? | Description |
| grant\_type | Mand | Value MUST be set to “client\_credentials” |
| client\_assertion\_type | Mand | Value MUST be set to “urn:ietf:params:oauth:client-assertion-type:jwt-bearer” |
| client\_assertion | Mand | A signed JWT, using JSON Web Signature – JWT payload details below in section 4.2 |

For example (non-normative):

POST /token HTTP/1.1

Host: auth.login.nhs.uk

Content-Type: application/x-www-form-urlencoded

grant\_type=client\_credentials&

client\_assertion\_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-type%3Ajwt-bearer&

client\_assertion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiIxMjM0NTY3ODkwIiwic3ViIjoiSm9obiBEb2UiLCJhdWQiOjE1MTYyMzkwMjIsImV4cCI6MTIzNDU1NjYsImp0aSI6IjIxMzI4NDU4LWRmZ2ZnaCJ9.4Tdu0hWTr1Fl03azjMtL2zcvWurx427q\_Y0meyHNahE

The client creates a client\_assertion, a JWT that is RSA-SHA512 signed with the pre-agreed RSA private key. This is as per section 4.

### Token Request Validation

References:

* JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants [1]
* Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants [2]

The Token Request is validated as described in JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants

### Token Response

#### Successful Response

References:

* JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants [1]
* Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants [2]

After receiving and validating a valid and authorized Token request from the client, the Token Endpoint returns a response which includes an Access Token. The response uses the “application/json” media type.

Table 2: Token Response: HTTP headers & values

|  |  |
| --- | --- |
| Header Name | Value |
| Cache-Control | no-store |
| Pragma | no-cache |

Table 3: Token Response

| Parameter | Description |
| --- | --- |
| access\_token | Signed JWT which encodes the Access Token, which is opaque to the client. |
| token\_type | Must be value “Bearer” |
| expires\_in | The lifetime in seconds of the access token.  The authorization server WILL provide the expiration time via the “exp” claim within the token, as per section 4.2 |

For example (non-normative):

HTTP/1.1 200 OK

Content-Type: application/json

Cache-Control: no-store

Pragma: no-cache

{

“access\_token”: “SlAV32hkKG”,

“token\_type”: “Bearer”,

“expires\_in”: 300

}

#### Error Response

References:

* RFC6749 – The OAuth 2.0 Authorization Framework [3], s5.2

If the Token Request is invalid or unauthorized, the Authorization Server constructs the error response. The parameters of the Token Error Response are defined as in Section 5.2 of OAuth 2.0 [RFC6749]. The HTTP response body uses the application/json media type with HTTP response code of 400.

The following is a non-normative example Token Error Response:

HTTP/1.1 400 Bad Request

Content-Type: application/json

Cache-Control: no-store

Pragma: no-cache

{

“error”: “invalid\_request”

}

Table 4: Token Error Response

|  |  |  |
| --- | --- | --- |
| Parameter | Req? | Description |
| error | Mand | Error code |
| error\_description | Opt | Human-readable ASCII encoded text description of the error |
| error\_uri | Opt | URI of a web page that includes additional information about the error |

Table 5: Error Codes for Authentication Error Response

|  |  |
| --- | --- |
| Code | Description |
| OAuth 2.0 error codes | |
| invalid\_request | The request is missing a required parameter, includes an unsupported parameter value (other than grant type), repeats a parameter, includes multiple credentials, utilizes more than one mechanism for authenticating the client, or is otherwise malformed. |
| invalid\_client | Client authentication failed (e.g., unknown client, no client authentication included, or unsupported authentication method).  The authorization server MAY return an HTTP 401 (Unauthorized) status code to indicate which HTTP authentication schemes are supported. If the client attempted to authenticate via the “Authorization” request header field, the authorization server MUST respond with an HTTP 401 (Unauthorized) status code and include the “WWW-Authenticate” response header field matching the authentication scheme used by the client. |
| invalid\_grant | The provided authorization grant (e.g., authorization code, resource owner credentials) or refresh token is invalid, expired, revoked, does not match the redirection URI used in the authorization request, or was issued to another client. |
| unauthorized\_client | The authenticated client is not authorized to use this authorization grant type. |
| unsupported\_grant\_type | The authorization grant type is not supported by the authorization server. |
| invalid\_scope | The requested scope is invalid, unknown, malformed, or exceeds the scope granted by the resource owner |

Provision Account Endpoint

References:

* RFC6749 – The OAuth 2.0 Authorization Framework [3], s4.1.3
* RFC6750: OAuth 2.0 Bearer Token Usage [4]

The Provision Account Endpoint is an OAuth 2.0 Protected Resource that enables the core provisioning of an End-User. The endpoint uses a REST-based standard with conventions for attribute names and interface behaviour.

The endpoint for User Provisioning is /provision-account. The endpoint currently provides single method for creating/amending user account.

The Access Token from the Client Credentials grant MUST be sent as a Bearer Token using the Authorization header field, as per OAuth 2.0 Bearer Token Usage [4].

This flow is used when a Service Consumer is requesting a create/amend a user account within the NHS login Platform. The endpoint messages involved are:

Table : Provision account endpoint details

|  |  |
| --- | --- |
| **Message to Endpoint** | **Description** |
| Create/Amend user account  POST /provision-account | User account is uplifted to high level of identity verification if the account already exists otherwise a new account is provisioned for user to claim later. |

The following sections details the Provision Account request and response after the Service Consumer has obtained an Access Token.

### Provision Account Request

Information below MUST be included within the body of the POST request, and the access token must be included in the header, as per The OAuth 2.0 Authorization Framework [3].

Table : Provision Account request parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Key** | **Req?** | **Value** | **Additional information** |
| nhs\_number | Mand | Citizen NHS number | The citizen’s NHS Number, which has been verified |
| email\_address | Mand | Citizen email address | The email address for the citizen. |
| date\_of\_birth | Mand | Citizen date of birth | MUST be in YYYY-MM-DD format |
| ods\_code | Mand | ODS code | MUST be the ODS code of the provisioner. A letter followed by 6 numbers |
| phone\_number | Mand | Citizen mobile number | MUST include the country code e.g. +447825428822 |

For example (non-normative):

POST /provision-account HTTP/1.1

Host: api.login.nhs.uk/provisioning

Content-Type: application/json

Authorization: Bearer h480djs93hd8

{

“nhs\_number”: “7545389484”,

“email\_address”: “test\_user@test.com”,

“date\_of\_birth”: “1993-17-12”,

“phone\_number”: “+44----------”,

“ods\_code”: “A00002”

}

### Provision Account Success Response

A successful provision account request will return a success response.

Table : Provision Account Success Response Structure

|  |  |  |
| --- | --- | --- |
| Parameter | Req? | Description |
| code | Mand | Success code |
| description | Opt | Human-readable ASCII encoded text description of the error |

Table : Provision Account Success Responses

|  |  |
| --- | --- |
| **Code** | **Description** |
| create | User able to create a new account |
| uplift | User able to uplift an existing account |

For example (non-normative):

HTTP/1.1 200 OK

{

“description”:”User able to create a new account”,

“code”:”create”

}

### Provision Account Error Response

An unsuccessful provision account request will return an error response.

Table : Provision Account Error Response Structure

|  |  |  |
| --- | --- | --- |
| Parameter | Req? | Description |
| code | Mand | Error code |
| description | Opt | Human-readable ASCII encoded text description of the error |

Table : Provision Account Error Responses

|  |  |
| --- | --- |
| Code | Description |
| 11000 | Service not available. |
| 11010 | Data in request not valid |
| 11021 | Service not supported for ODS code provided |
| 11011 | Too many requests from ODS code |
| 11001, 11002, 11006, 11007, 11008, 11009, 11018, 11019 | Unable to provision account for user |
| 11005 | User already has P9 account |
| 11004 | Unable to provision account for user email already in use |
| 11003 | User already has a pending provision account request from within last 7 days. |

**Note**: The error descriptions are for the Service Consumer and are not suitable for an end user.

For example (non-normative):

HTTP/1.1 400 ERROR

{

“description”:” Unable to provision account for user email already in use”,

“code”:” 11004”

}

# Tokens

## JWT for Client Authorization

References:

* RFC7519 – JSON Web Token (JWT) [5]
* RFC7515 – JSON Web Signature (JWS) [6]

The JWT token for client authorization consists of three parts: a header, a payload, and a signature.

### Token Header

The JWT header will contain the following claims:

Table 12: JWT Header

| Claim | Req? | Name | Description |
| --- | --- | --- | --- |
| alg | Mand | Algorithm used for signing the JWT | “RS512” – RSASSA-PKCS1-v1\_5 with the SHA-512 hash algorithm |
| typ | Mand | Type | “JWT” |

### Token Payload

References:

* RFC7523 - JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants [1]

Table 13: Assertion token claims

| Parameter | Req? | Example | Description |
| --- | --- | --- | --- |
| iss | Mand | myClientIdentifier1 | The identifier for the client system, as registered with the NHS login platform |
| sub | Mand | myClientIdentifier1 | The identifier for the client system, as registered with the NHS login platform |
| aud | Mand | https://auth.login.nhs.uk/token | The NHS login platform token URL |
| exp | Mand | 1311281030 | Time the JWT will expire. The client SHOULD set this to a value appropriate to the security and efficiency context in which the client is operating |
| jti | Mand | heefdfriewewpf..ff | JWT unique identifier. Value is unique to each token created by the issuer. NHS login will utilise the value in this claim to protect against replay attacks. |

### JWT Signature

References:

* RFC7519 – JSON Web Token (JWT) [5]
* RFC7515 – JSON Web Signature (JWS) [6]

The JWT signature consists of the contents of the header and payload, signed with your private key.

## Access Token Payload

References:

* Access Tokens and Audit (JWT) [7]

Table 14: Access token claims

|  |  |  |
| --- | --- | --- |
| Parameter | Example | Description |
| iss | <https://auth.login.nhs.uk/> | The NHS login platform issuer identifier |
| sub | myClientIdentifier1 | The identifier for the client system, as registered with the NHS login platform |
| aud | myClientIdentifier1 | The identifier for the client system, as registered with the NHS login platform |
| iat | 1311280970 | Time the JWT was created |
| exp | 1311281030 | Time the JWT will expire. This claim MUST be used by clients to determine when new a new Access Token needs to be requested |

## JWT Signing

References:

* RFC7519 – JSON Web Token (JWT) [5]
* RFC7515 – JSON Web Signature (JWS) [6]

All JWTs MUST be signed using the RSASSA-PKCS1-v1\_5 with the SHA-512 hash algorithm (“RS512”).

# References

|  |  |
| --- | --- |
| [1] | Internet Engineering Task Force (IETF), “RFC7523 - JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants,” [Online]. Available: https://tools.ietf.org/html/rfc7523. |
| [2] | Internet Engineering Task Force, “RFC7521: Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants,” [Online]. |
| [3] | Internet Engineering Task Force (IETF), “RFC6749 - The OAuth 2.0 Authorization Framework,” [Online]. Available: https://tools.ietf.org/html/rfc6749. |
| [4] | Internet Engineering Task Force (IETF), “RFC6750: OAuth 2.0 Bearer Token Usage,” [Online]. Available: https://tools.ietf.org/html/rfc6750. |
| [5] | Internet Engineering Task Force (IETF), “RFC7519: JSON Web Token (JWT),” [Online]. Available: https://tools.ietf.org/html/rfc7519. |
| [6] | Internet Engineering Task Force (IETF), “RFC7515 - JSON Web Signature (JWS),” [Online]. Available: https://tools.ietf.org/html/rfc7515. |
| [7] | NHS Digital, “Access Tokens and Audit (JWT),” [Online]. Available: https://developer.nhs.uk/apis/spine-core/security\_jwt.html. |
| [8] | Internet Engineering Task Force (IETF), “RFC3339 - Date and Time on the Internet: Timestamps,” [Online]. Available: https://www.ietf.org/rfc/rfc3339.txt. |
| [9] | Cabinet Office, “GPG44 - Authentication credentials for online government services,” [Online]. Available: https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services. |
| [10] | Cabinet Office, “GPG45 - Identity proofing and verification of an individual,” [Online]. Available: https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual. |
| [11] | NHS Digital, “DCB3051 Identity Verification and Authentication Standard for Digital Health and Care Services,” [Online]. Available: http://digital.nhs.uk/isce/publication/dcb3051. |