



ONE Access Gateway - Transport Specification

Version 1.0

January 2020

Copyright Notice

Copyright © 2020, Ontario Health (Digital Services)

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Ontario Health (Digital Services). The information contained in this document is proprietary to Ontario Health (Digital Services) and may not be used or disclosed except as expressly authorized in writing by Ontario Health (Digital Services).

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

APPROVER(S)	TITLE/DEPARTMENT	APPROVED DATE
-------------	------------------	---------------

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
0.1	2019-08-06	Document drafted	eHealth Ontario
0.2	2019-10-08	Edits and additional contents added following review with internal stakeholders	eHealth Ontario
1.0	2020-01-09	Updated following review with external stakeholders	Ontario Health (Digital Services)

Contents

1.0	Introduction	1
1.1	About This Document.....	1
2.0	Architecture Overview	2
3.0	Client Application Registration.....	3
4.0	Obtain Access Token and ID Token	4
5.0	Invoke API.....	5
5.1	Gateway Response Codes	5
5.2	HTTP Headers	7
5.3	Request Tracking	7
6.0	Versions	9
6.1	Versian Syntax	9
6.2	Versian Changes	9
6.3	Multiple Subscribed Versions.....	9
7.0	API Product Life Cycle	10
8.0	Environments.....	11
9.0	Glossary.....	12
10.0	Quick Links.....	12

1.0 Introduction

1.1 About This Document

The primary audience for this integration guide includes Clients of Ontario Health (Digital Services) with an interest in ONE Access Provider Gateway integration. The document assumes the reader has technical knowledge of the ONE Access Gateway, Application Programming Interfaces (APIs) and API Management Solutions such as IBM API Connect. The document provides technical instructions for adopters (API Consumers (Client Applications)) to follow in order to consume APIs exposed by the ONE Access Provider Gateway after completing the required technical and project prerequisites to expedite the integration process and minimize potential impediments.

Client Applications wishing to integrate with the ONE Access Provider Gateway will be required to comply with legal, privacy, security and project requirements, which will be provided at project initiation.

2.0 Overview

The ONE Access Provider Gateway exposes a set of RESTful FHIR APIs protected by OAuth2/Open ID Connect authorization and authentication protocols.

After completing the required project prerequisites, the following tasks should be completed by the Client Application before interacting with the gateway:

1. Register the Client Application;
2. Obtain an access token and identity token from the eHealthOntario ONE ID framework;
3. Invoke the APIs exposed by gateway, and receive response.

Each of the steps above are described in detail in this document.

3.0 Client Application Registration

Every Client Application needs to be registered in order to interact with the ONE Access Provider gateway as outlined below.

Registration Activities

The following registration activities must be performed for each environment in which a connection is made, including the Partner Self-Test Environment and Production environments:

1. **Create Client organization:** The registration is performed by Ontario Health (Digital Services) on behalf of the Client Application organization.
2. **Create Client Application:** This step is performed by Ontario Health (Digital Services) on behalf of the Client Application organization. At the end of successful Application registration, the following information is returned to the Client Application organization:
 - a. Gateway Client ID (API)
 - b. Gateway Client secret (Optional, only for trusted clients)
3. **Subscribe to product:** The Client Application created above must be subscribed to a specific API product before it can be used. In order to do so, Ontario Health (Digital Services) on behalf of the Client Application organization subscribes the appropriate API product to a Client Application. Once subscribed, the Client Application is ready to invoke the APIs of the selected API product via the ONE Access Provider Gateway. The following information will be available after a successful subscription:
 - a. API product name and version information;
 - b. API gateway endpoint for the selected product.

Note:

The information above describes the current state Client Application registration process, where the API Client registration workflow is not integrated with the OAuth2 Client registration process.

The above activities will be conducted by Ontario Health (Digital Services) staff members through manual and semi-automated processes.

- At the start of the process, all the information needed for organization and Application registration at the ONE Access Gateway and OAuth2 subsystem is collected.
- The registration is completed in the API Manager, the resulting API key and secret are transmitted to the OAuth2 system; to provision their system for token creation.
- The output of the process is securely transferred to client application organizations.

4.0 Obtain Access Token and ID Token

An access token is required to invoke an API exposed by the ONE Access Gateway. Follow ONE ID OAuth2/OIDC guidelines described in the link below to obtain an access token. Depending on the Client type and the access mechanism, a ONE ID user account may be needed to obtain an access token with appropriate scope and selected profile.

[ONE ID OpenID Connect Specification](#)

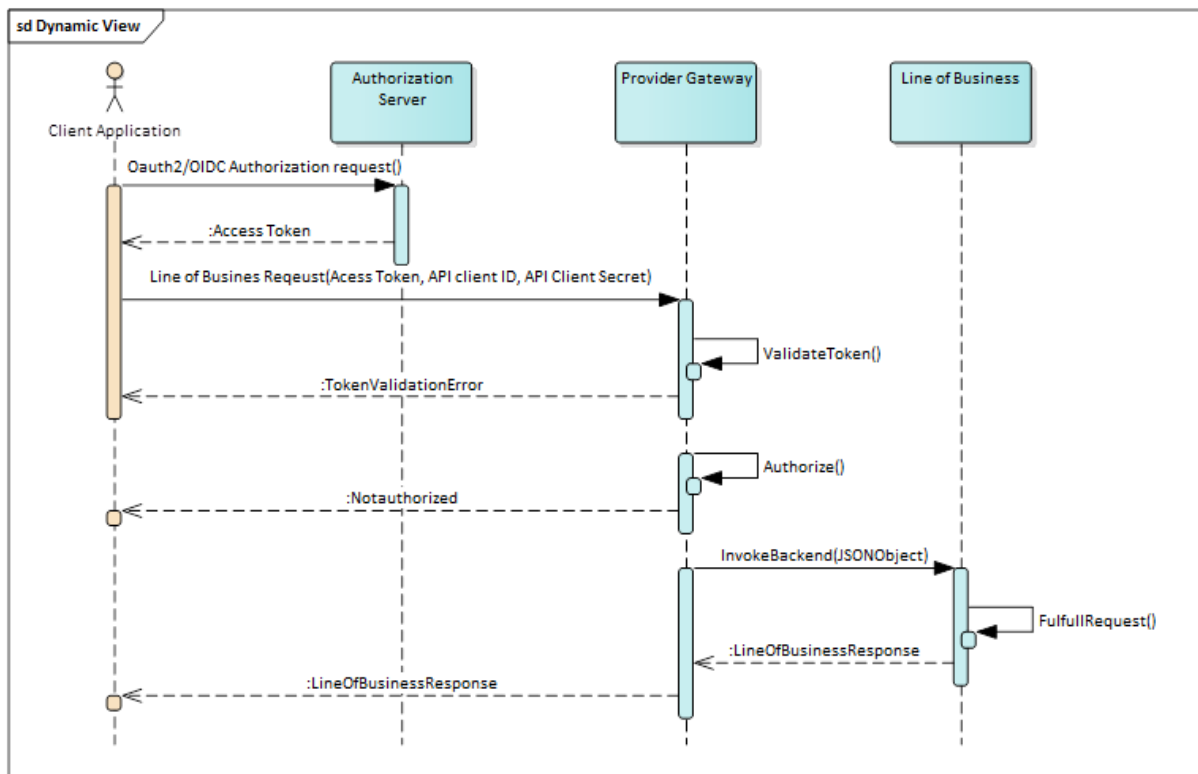
At present gateway expects callers to have a valid OAuth2 token with proper scopes to access an API. Any existing clients who use ONE ID SAML based login flows, would need to initiate a new OIDC flow as described in the above specification to obtain a new access token before accessing the gateway. This will enable SAML based clients to obtain a token without needing to re-enter the user credentials if they have already logged in.

The access token returned to the Client Application is meant to be used for API calls by the Client Application at the ONE Access Gateway. The Client Application is expected not to modify or depend on data within the token, as the token format may change. The audience of the token is the ONE Access Provider Gateway, not the Client Application.

5.0 Invoke API

The access token obtained in the previous step is used as a bearer token to invoke the selected RESTful API. The bearer token is placed within the authorization header of the http request as defined in ([Tools.ietf.org, 2019](https://tools.ietf.org/html/rfc6750)).

http request header,
Authorization: Bearer <access token>



5.1 Gateway Response Codes

The table below lists http response codes returned by the ONE Access Provider Gateway. Please note that the API may return status codes in addition to the ones listed below as part of business processing. Client Application developers will be provided, and are required to review, API-specific documentation (such as the FHIR Standards, as applicable to integration project) to understand all possible HTTP codes returned as part of API interaction.

HTTP Code	Description
200/201	No system errors from the ONE Access Provider Gateway point of view; however, there could be business errors, warnings or information messages. In case of business errors or warnings, FHIR OperationOutcome is populated with appropriate information.

HTTP Code	Description
400	Bad request - Token not present - Back-end token validation failed
401	Unauthorized - Invalid Client ID - Invalid Client ID and secret - Required scope not available - Required profile not available - Token expired - Issued in future - Not destined for gateway - Not issued by ONE ID - Required claims for the gateway processing is not present - Back-end fine grained authorization failed - API keys in the token goes not match with the ones used in the request
404	Resource not supported by ONE Access Provider Gateway.
405	Method not allowed as per business rules.
500	Internal Error - Back-end error - Default timeout for backend connectivity is set o 60 seconds - JWT cannot be validated, signature issues

5.2 HTTP Headers

The table below outlines the number of http headers that are used within the ONE Access Provider Gateway. Some are required to be filled by the Client Application placing the API request, while others are populated by the ONE Access Provider Gateway, as described below.

Header name	External Request	Gateway to LOB request	LOB to gateway response	External response
X-Gtwy-Client-Id	Identifies the Client identifier	Not present	Not present	Not present
X-Gtwy-Client-Secret	Specifies the Client secret	Not present	Not present	Not present

5.3 Request Tracking

There is a need to track end-to-end requests and responses within the ONE Access Provider Gateway. The early version of the gateway used its own http headers (GtwyTxId, LOB.transactionid) to track transactions through the system.

However, HL7 FHIR R4 has provided recommendation on this area as described [here](#). This approach is preferred to be adopted in order to be more aligned with the standard.

In addition to the headers mentioned in the standard, two custom headers are proposed to achieve the end-to-end transaction tracking capability as shown in the table below.

The ONE Access Provider Gateway always propagates any header present in the Client Application request to the API backend. Inbound request headers are marked as optional in order to avoid any request rejection if a header is not present.

Header name	External Request	Gateway to Backend request	Backend to gateway response	External response
X-Request-Id	Identifies the Client transaction ID. Optional.	Identifies the Client transaction ID. Optional.	Not present	Identifies the gateway transaction ID. Mandatory.
X-Correlation-Id	Not present	Not present	Not present	Identifies the original X-Request-Id in the Client request.
X-Forwarded-For	Not present	Identifying the IP address of the requester. Optional.	Not present	Not present
X-Forwarded-Host	Not present	Identifies the original requested host	Not present	Not present
X-Intermediary	Not present	Identifies the Gateway. Optional.	Not present	Not present
X-GtwyTxId	Not present	Identifies the gateway global transaction ID.	Not present	Not present
X-LobTxId	Not present	Not present	Identifies the line of business transaction ID.	Identifies the line of business transaction ID.

6.0 Versions

6.1 Version Syntax

API Products contain one or more APIs. These APIs and API Products follow a three-part version schema, i.e., `<Major>.<minor>.<revision>.<build>` all represented in digits, starting with 1.0.0.0 Revisions are generally defect fixes and minor feature enhancements with backward compatibility. Minor digits signify a business feature support (which may or may not be backward compatible), while major digits represent major business changes, and are usually not backward compatible.

6.2 Versions Changes

Any change to an API version results in a corresponding change to a section of the API product. For this reason, only API product version changes are discussed in this document, not API version changes.

Once Clients subscribe to a specific API product version, they will continue to consume the subscribed API product version without any impact from subsequent version changes of the API product, subjected to following:

- API product owners (Ontario Health (Digital Services)) will automatically migrate the Client to a later version of the API product after determining the new API product version is backward compatible with the subscribed API product version. This migration will have no impact on the Client side and no action is necessary from the Client Application.
- When the new API product is not backward compatible with the subscribed version, client application owners can subscribe to the new product version once necessary development and testing has been completed against the new product version. Subscription upgrade may be carried out at the product owners' discretion or requested by Ontario Health (Digital Services).
- Ontario Health (Digital Services) may request consumers to upgrade to a newer version when old versions are no longer supported.

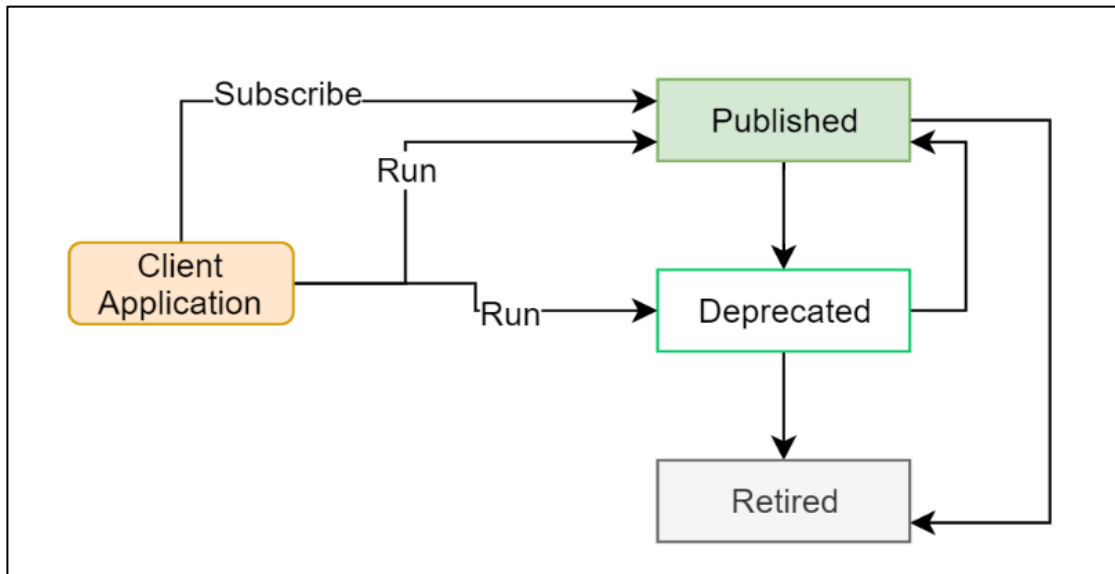
Application owners have the ability to go back to an older version of the API product if it is still available for subscription.

6.3 Multiple Subscribed Versions

If Clients want to subscribe to and consume two different versions of the same API product, two different API keys should be used. Otherwise, all Client requests will be forwarded to the first subscribed version of the API product.

7.0 API Product Life Cycle

The following diagram illustrates the API Product Life Cycle from the point of view of the consumer Application. The two key states are “Published” and “Deprecated”. Clients can only subscribe to published API products; clients of deprecated API products can continue to function, but no new subscriptions are allowed.



8.0 Environments

External Client applications wishing to integrate with the ONE Access Provider Gateway are required to comply with legal, privacy, security and project requirements which will be provided at project initiation. Once the appropriate prerequisites are met, Client Applications are connected to two environments:

- **Partner Self Test (PST)** for partner development, self-testing and conformance testing, using fabricated data.
- **Production (Prod)** for live use of real data in production.

Ontario Health (Digital Services) will not offer performance testing environments to external clients.

Name	Base Gateway Endpoint	Description
Partner Self Test (PST)	https://provider.pst.ehealthontario.ca	• Environment for partner development, self testing and conformance testing • Fabricated data.
Production (prod)	https://provider.ehealthontario.ca	• Production environment • Real data.

9.0 Glossary

1. **Access Token** - The access token verifies that your Application is authorized to access the requested resource. Use the Client ID and Client secret to exchange an access token at the token endpoint.
2. **API Key** - One type of credential that supports third party API authorization.
3. **API Product** - API products are bundled APIs (resources and service plan), that are made available to app developers for consumption.
4. **Application Program Interface (API)** - A set of standard software interrupts, calls, functions, and data formats that can be used by an Application program to access network services, devices, Applications, or operating systems.
5. **Authentication** - In computer security, verification of the identity of a user or process and the construction of a data structure that contains the privileges that were granted to the user or process.
6. **FHIR** - Defines a set of resources for health. These resources represent granular clinical concepts that can be exchanged to quickly and effectively solve problems in healthcare and related process. The resources cover the basic elements of healthcare - patients, admissions, diagnostic reports, medications, and problem lists, with their typical participants, and also support a range of richer and more complex clinical models. The simple direct definitions of the resources are based on thorough requirements gathering, formal analysis and extensive cross mapping to other relevant standards.
7. **OAuth** - An HTTP-based authorization protocol that gives Applications scoped access to a protected resource on behalf of the resource owner, by creating an approval interaction between the resource owner, Client, and resource server.
8. **ONE ID** - Ontario Health (Digital Services)'s identity and access management solution. It provides and manages digital credentials for clinicians, brokers a federated identity platform enabling providers to leverage existing credentials, and implements a province-wide single sign on solution for the provincial digital health record. It also delivers a number of additional capabilities (e.g. authorization, risk-based authentication).
9. **Open IDConnect (OIDC)** - An identity protocol and open standard that is built on top of the OAuth 2.0 protocol. It enables Client Applications to rely on authentication that is performed by an OpenID Connect provider to verify the identity of a user.
10. **RESTful API** - FHIR is described as a 'RESTful' specification based on common industry level use of the term REST. In this RESTful framework, transactions are performed directly on the server resource using an HTTP request/response. The API does not directly address authentication, authorization, and audit collection.

10. Relevant Links

This section lists and hyperlinks all the documents that are external to the guide.

1. (2006). Himss dictionary of healthcare information technology terms, acronyms, and organizations. Chicago, IL: HIMSS.
2. Canadian FHIR Registry. Retrieved from <https://simplifier.net/organization/CanadianFHIRRegistry/~projects>
3. IBM API Connect. Retrieved from <https://www.ibm.com/ca-en/marketplace/api-management>
4. IBM Cloud Identity. (n.d.). Retrieved from <https://www.ibm.com/support/knowledgecenter/en/SSCT62/com.ibm.iamservice.doc/glossary/glossary.html>
5. Introduction: Apigee Docs. (n.d.). Retrieved from <https://docs.apigee.com/api-platform/publish/what-api-product>
6. Resource OperationOutcome - Content. (n.d.). Retrieved from <https://www.hl7.org/fhir/operationoutcome.html>
7. The OAuth 2.0 Authorization Framework: Bearer Token Usage. [online] Available at: <https://tools.ietf.org/html/rfc6750> [Accessed 10 Sep. 2019].