EMR EHR Connectivity 2.0

Provincial Gateway – Business View

December 23, 2019

Document Version & Status: 1.0 – DFC (Draft for Comment)

Table of Contents

1. INTRODUCTION 3

1.1 OVERVIEW 3

1.1.1 What is the Provincial Gateway? 3

1.1.2 What is Open Authorization 2.0? 3

1.2 MODELS OF AUTHORIZATION IN THE PROVINCIAL GATEWAY 4

2. SYSTEM VIEW 5

2.1 PROVINCIAL GATEWAY INTERACTIONS 5

2.2 PROVINCIAL GATEWAY PARAMETERS 5

3. APPENDIX A: GLOSSARY OF KEY TERMS AND DEFINITIONS 7

3.1 ACRONYMS AND ABBREVIATIONS 7

3.2 DEFINITIONS 8

1. INTRODUCTION

1.1 Overview

The Ontario Health ONE Access Provider Gateway (Provincial Gateway) is a modernized platform for enabling the integration of client applications (e.g., EMR Offerings) with provincial clinical repositories and registries in a secure and reliable manner. It is a solution to better support the client applications to access EHR data through following a standards-based approach. All EHR products and services hosted on the Provincial Gateway support OAuth2 and OIDC for authentication and authorization.

1.1.1 What is the Provincial Gateway?

The Provincial Gateway enables client applications (e.g., EMR Offerings) to connect to and access EHR products and services using a standards-based approach to access data with flexibility and ease of use for developing solutions utilizing the HL7 FHIR standard.

1.1.2 What is Open Authorization 2.0?

Open Authorization 2.0 (OAuth2), with OpenID Connect (OIDC) as the identity layer, is an authorization framework utilized by the Provincial Gateway to authenticate and authorize the client applications (e.g., EMR Offerings) and their users' access to various EHR products and services available.

1.2 Models of Authorization in the Provincial Gateway

Depending on the EHR product or service and the business policies that govern it, each EHR product or service will follow different methods for the authorization of access to the EHR data. For example, some EHR products or services grant access to EHR users explicitly, whereas other EHR products or services may grant access to a clinic organization that implicitly includes any EHR users that are part of that clinic organization.

The following provides a high-level view of the different methods of authorization that may be used to connect to the Provincial Gateway and to EHR services. (The process to register an EMR or an EMR user for access to these resources is managed by Ontario Health which is beyond the scope of this document.)

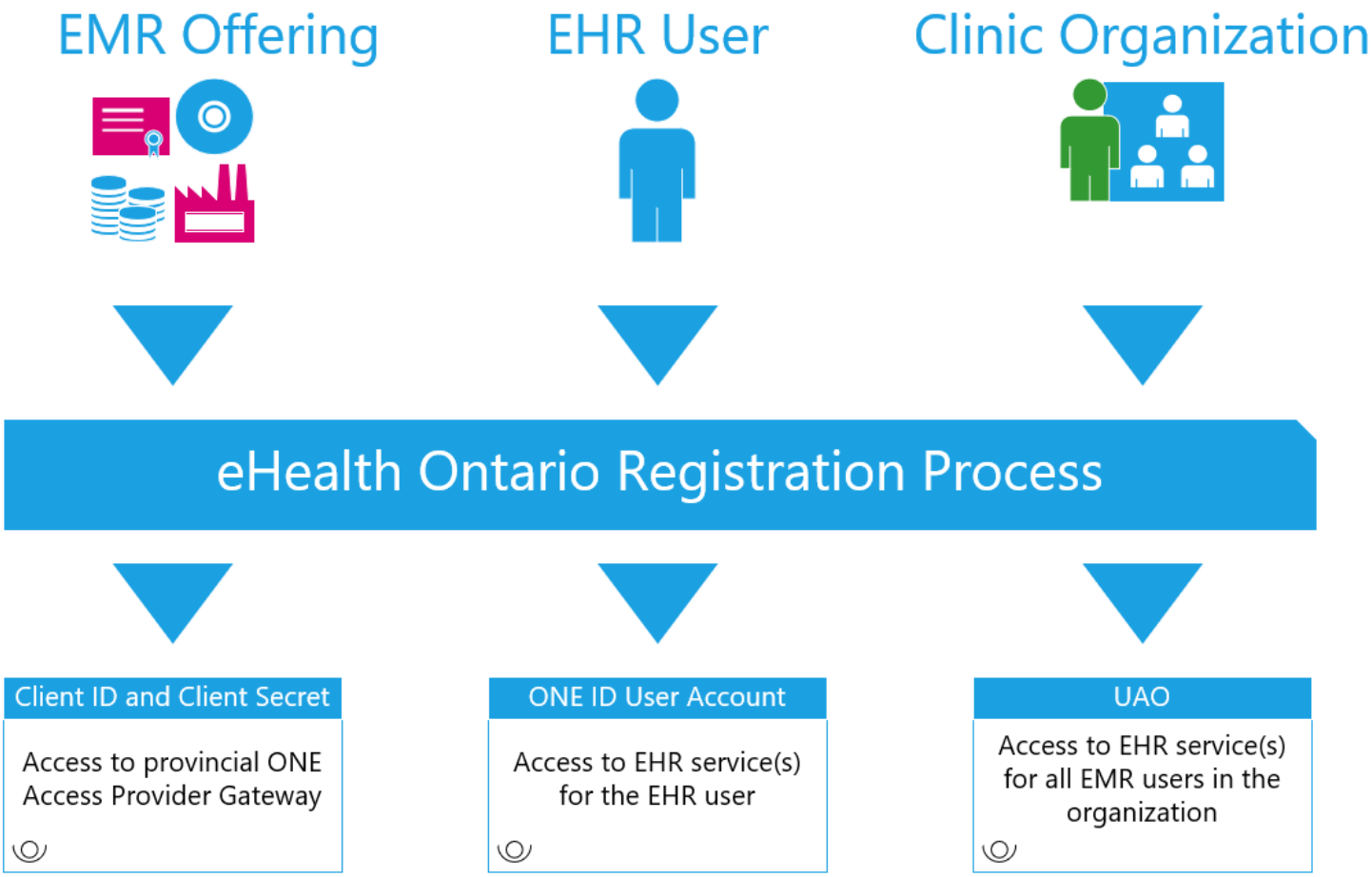


Figure 1 - Models of Authorization in the Provincial Gateway

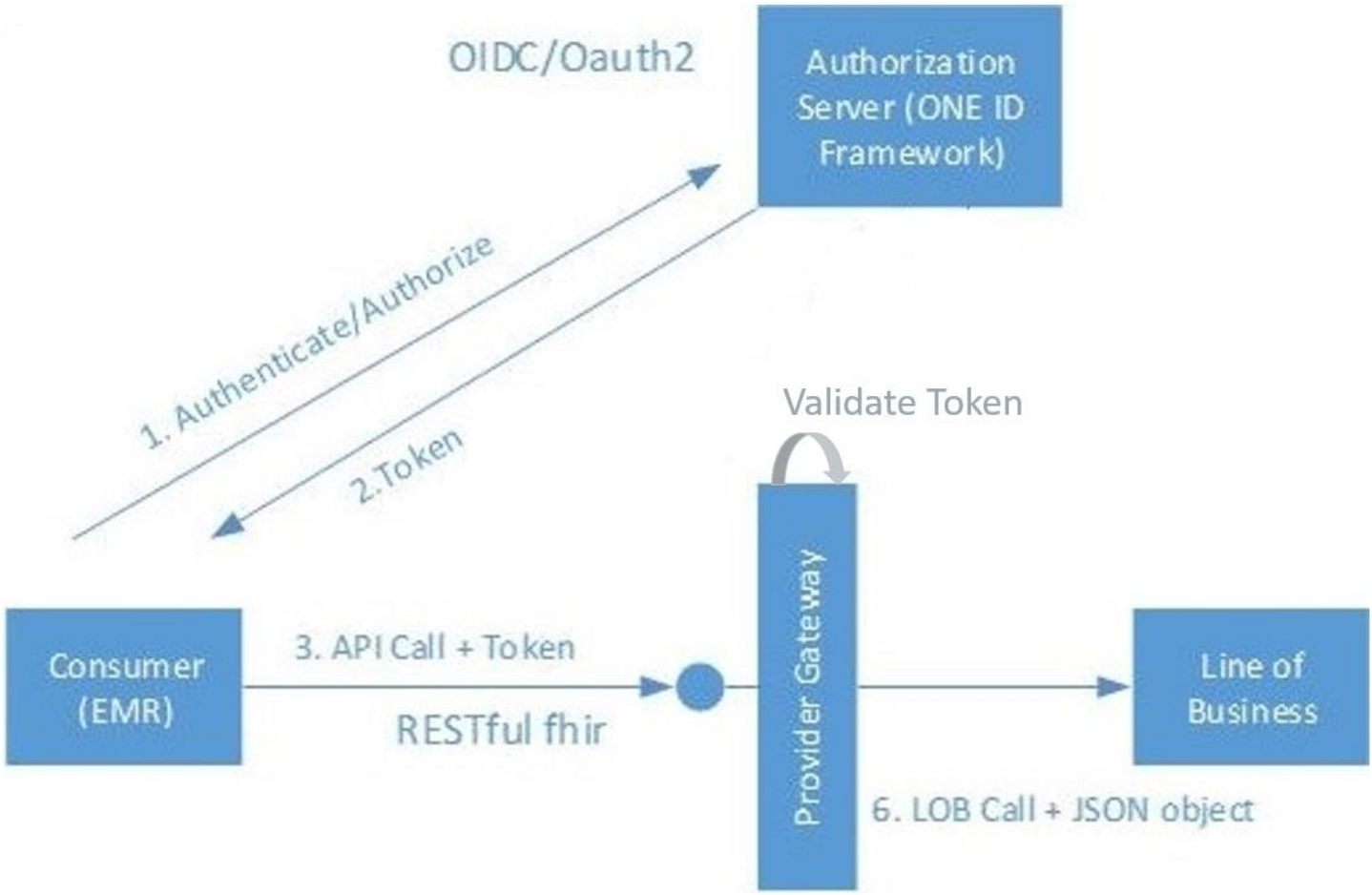
2. SYSTEM VIEW

2.1 Provincial Gateway Interactions

The following diagram provides a high-level overview of the role of the Provincial Gateway, which acts as the protected resource for client applications (i.e., consumers) wishing to access HER assets.

The API gateway will:

1. Accept and validate bearer tokens
2. Validate that signature from the token is from the ONE ID OIDC/OAuth2 service
3. Accept only valid tokens from the ONE ID OIDC/OAuth2 service
4. Check the audience claim to ensure that it includes the API Provider Gateway Identifier
5. Validate Token
6. Call Line of Business (LOB) - Interpret Access Tokens using JSON web token (JWT)



2.2 Provincial Gateway Parameters

The following table outlines the message header information that an EMR Offering needs to provide in order to authenticate and connect to the Provincial Gateway.

ID	NAME	DEFINITION	CARDINALITY
1	X-Gtwy-ClientId	The Gateway Client ID uniquely identifies each EMR tenant that is registered to connect to the Provincial Gateway. It is assigned to each EMR tenant during the Ontario Health registration process and is used to identify registered EMR tenants.	1..1
2	X-Gtwy-Client-Secret	The Gateway Client Secret is used to provision the EMR tenant for token creation. It is assigned to each EMR tenant during the Ontario Health registration process. And is used to authenticate registered EMR tenant.	1..1
3	X-Request-Id	The Client Transaction ID is generated by the EMR Offering to uniquely identify each message sent by the EMR Offering and interacting with the Provincial Gateway. The Provincial Gateway will respond with a corresponding Gateway Transaction ID, to be used for troubleshooting, logging and auditing purposes between the two systems (and also the EHR service).	1..1
4	X-LobTxId	The Line of Business ID uniquely identifies each EHR service. It will be provided by the Provincial Gateway and may be required to be provided back by the EMR Offering to identify which EHR service the message or transaction relates to. For example, the EHR Service ID is used when setting the patient context to identify which EHR service is to use that patient context.	0..*

3. APPENDIX A: GLOSSARY OF KEY TERMS AND DEFINITIONS

3.1 Acronyms and Abbreviations

This table identifies definitions for terms used within or that are relevant to this document.

ACRONYM	DEFINITION
API	Application Programming Interface
DHDR	Digital Health Drug Repository
DHIR	Digital Health Immunizations Repository
EHR	Electronic Health Record
EMR	Electronic Medical Record
FHIR	Fast Healthcare Interoperability Resources
HIC	Health Information Custodian
HL7	Health Level Seven
IETF	Internet Engineering Task Force
JSON	JavaScript Object Notation
JWT	JSON web token
OAuth2	Open Authentication 2.0
OH	Ontario Health (formerly eHealth Ontario)
OIDC	OpenID Connect
OIDF	The OpenID Foundation
PEM	Privacy Enhanced Mail
ReST	Representational State Transfer
SSO	Single Sign-On
UAO	Under the Authority of
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

3.2 Definitions

The following are the terms and definitions used to describe the concepts used in this document.

TERM	DEFINITION
EMR tenant	A tenant applies to an EMR used by an individual or a group of people. For example, a tenant could be a single-family physician or a family health team comprised of many EMR users and distributed across several clinics.
EMR user	A user who has access rights to log into an EMR. This can be an end-user, an administrative user who administers the EMR, or any other user of the EMR. They may or may not also have access to an EHR service.
EHR user	A user who has access rights to one or more EHR services. Typically, an EHR user is also an EMR user.
Gateway Client ID	The Gateway Client ID is the information assigned as part of an Ontario Health process to register an EMR Offering instance to allow it to connect to the Provincial Gateway as part of the OAuth2 interaction. It uniquely identifies the EMR Offering instance and is provided by the EMR as part of the interaction when connecting to the Provincial Gateway.
Gateway Client Secret	The Gateway Client Secret is a private key used to authenticate a registered EMR Offering to connect to the Provincial Gateway. It should be kept confidential and stored securely.
Gateway endpoint	This is the URL for the EMR Offering to connect to the Provincial Gateway. This value will be different for differing environments (e.g., a test vs. production environment).
PEM	It is a Base-64 encoded X.509 certificate. In the context of the Provincial Gateway, it is used to validate the signature of a JWT.
Under the Authority of (UAO)	This information defines the HIC or organization of which: a) clinic practice is authorized to act on behalf b) an EMR user is authorized to act on behalf The UAO is assigned by Ontario Health as part of a registration process for a user to receive a ONE ID account, as well as for an EMR Offering instance to receive a Gateway Client ID. An EMR user and/or a clinic may be assigned zero, one, or multiple UAO values. A user or clinic who has not successfully completed registration, or who does not belong to an organization would not be assigned a UAO. An EMR user who works at a single organization, or a clinical practice that operates under a single organization would be assigned one UAO, and a user or clinic practice that functions under multiple organizations would be assigned multiple UAO values respectively. Multiple EMR Offering instances or users working for the same organization would be assigned the same UAO. An EHR service, depending on its function, may rely on the UAO of the EMR user (where access is user-based), or the UAO of the clinic (if it is system-based), or a combination of them.

TERM	DEFINITION
	As a result, an EMR Offering instance needs to be assigned at least one UAO to connect to the Provincial Gateway. Similarly, an EMR user needs to be assigned at least one UAO to access an EHR service hosted on the Provincial Gateway.