Internet User Authorization (IUA)

Overview

The Internet User Authorization (IUA) is an interoperability profile that provides an authorization profile for the HTTP RESTful transactions. Being authorized means that the user, patient, or provider has legitimate access to this HTTP RESTful service. The authorization includes identifying the user and the application that is making the request to the HTTP RESTful server, so that server can make further access control decisions.

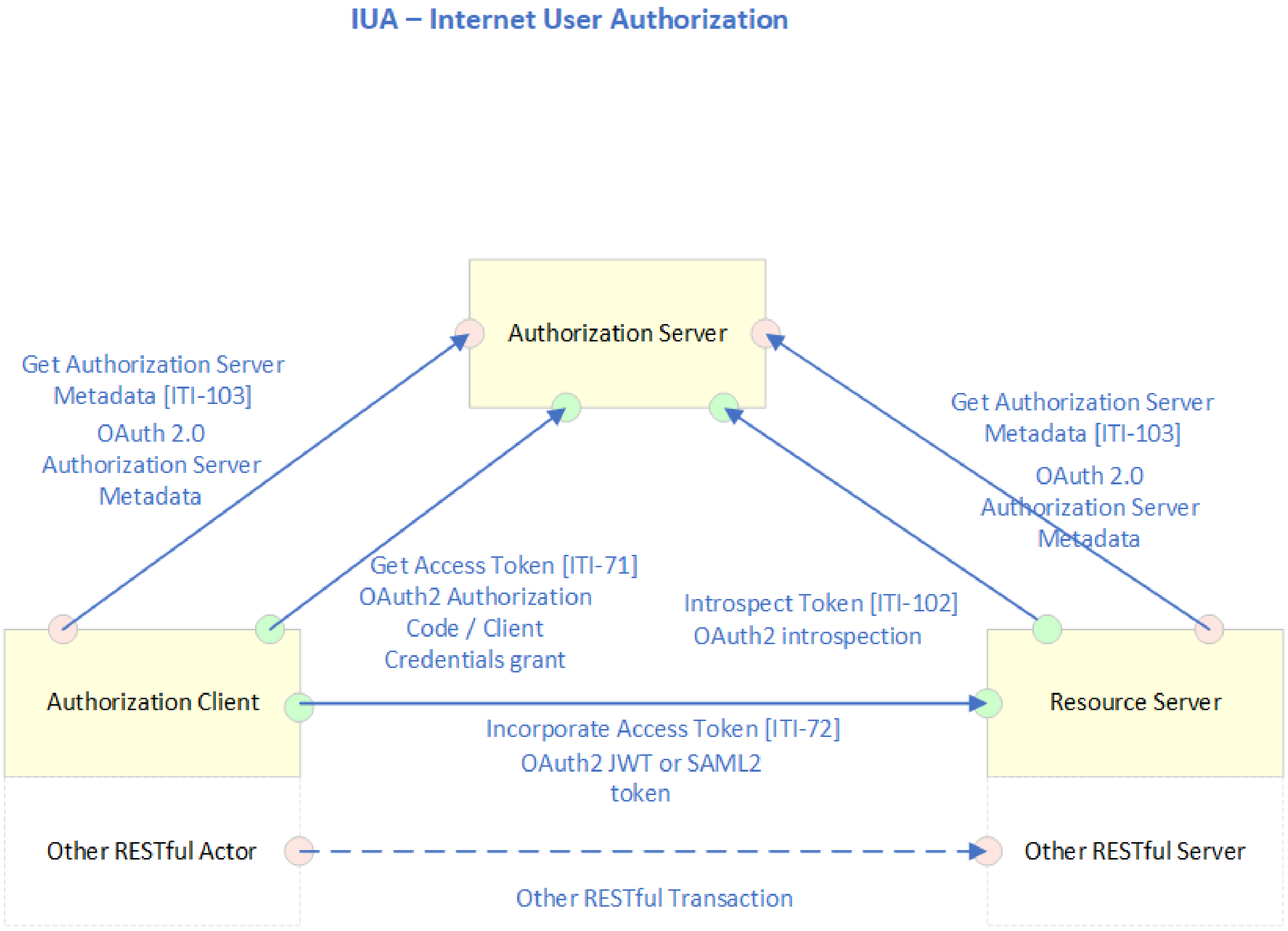
IUA conveys User Identity, Attributes, and Authorizations to a RESTful service to enable security and confidentiality policy enforcement. The primary use cases are for obtaining authorization for access to a resource using HTTP RESTful HTTP transactions. There are other use cases for delegation, provisioning, etc. which are out of scope for this profile.

The authorization service is separated from the HTTP RESTful access so that it can be provided by a different organization or part of the organization than the resource service. This is driven by the requirements of patients, providers, and other users to simplify and maintain autonomy and control over authorization services. A user may interact with dozens of providers. It is difficult for the user to coordinate different authorization mechanisms with each of these dozens of providers.

This pattern is a common Internet usage and there are already vendors of authorization services that are being used to solve this problem. These include Facebook, Google, and a variety of other service providers in different commercial and governmental sectors. Some countries may use their citizen identity card to access their governmental services. These overlap with providers of authentication services. These services allow a patient to establish an authentication and authorization relationship with minimal provisioning by the healthcare provider. The user can specify “use vendor X” to their healthcare provider.

Actors and Transactions

The following diagram provides an overview of the IUA profile Actors, Transactions and their interactions.


IUA – Internet User Authorization
Authorization Server
Get Authorization Server Metadata [ITI-103]
OAuth 2.0 Authorization Server Metadata
Get Authorization Server Metadata [ITI-103]
OAuth 2.0 Authorization Server Metadata
Get Access Token [ITI-71]
OAuth2 Authorization Code / Client Credentials grant
Introspect Token [ITI-102]
OAuth2 introspection
Authorization Client
Resource Server
Incorporate Access Token [ITI-72]
OAuth2 JWT or SAML2 token
Other RESTful Actor
Other RESTful Server
Other RESTful Transaction

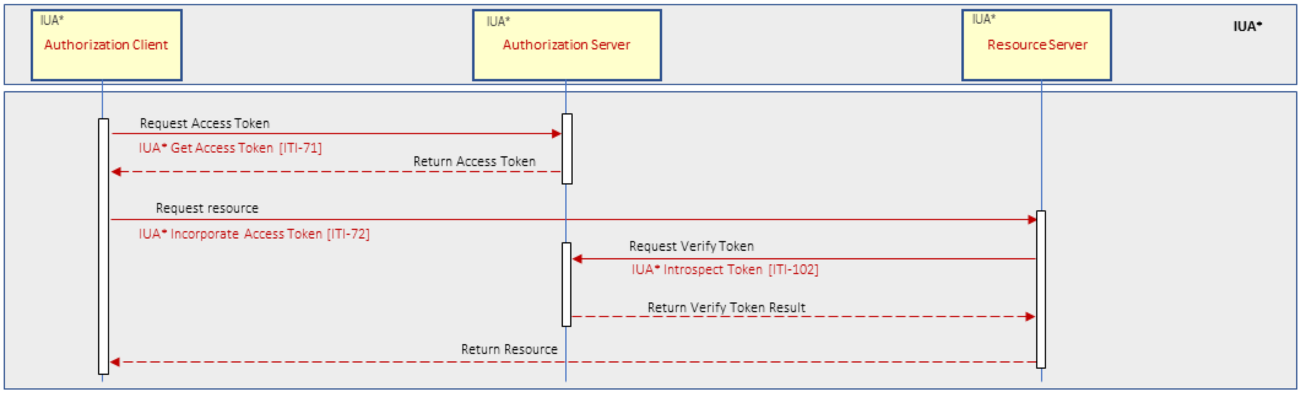
The table below lists the transactions for each actor directly involved in the IUA profile. To claim compliance with IUA, an actor shall support all required transactions (labeled “R”) and may support the optional transactions (labeled “O”).

Actor	Transaction	Optionality
Authorization Client	Get Access Token [ITI-71]	R
	Incorporate Access Token [ITI-72]	R
	Get Authorization Server Metadata [ITI-103]	O
Authorization Server	Get Access Token [ITI-71]	R
	Get Authorization Server Metadata [ITI-103]	O
	Introspect Token [ITI-102]	O
Resource Server	Incorporate Access Token [ITI-72]	R
	Get Authorization Server Metadata [ITI-103]	O
	Introspect Token [ITI-102]	O

Transactions

- Get Access Token [ITI-71] - This transaction is used by an Authorization Client to retrieve an OAuth 2.1-compliant access token. Uses RFC6749 - OAuth2.1 protocol and RFC7519 – JSON Web Token and JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens.
- Incorporate Access Token [ITI-72] - This transaction is used to incorporate authorization information into HTTP RESTful transactions. Uses RFC6749 - OAuth2.1 protocol.
- Introspect Token [ITI-102] - Token introspection defines a protocol that allows Resource Servers to query the Authorization Server to determine the set of claims for a given token that was presented to them by an Authorization Client. These claims include whether the token is currently active and the authorization context in which the token was granted.

Sequence Diagram


IUA*
Authorization Client
IUA*
Authorization Server
IUA*
Resource Server
IUA*
Request Access Token
IUA* Get Access Token [ITI-71]
Return Access Token
Request resource
IUA* Incorporate Access Token [ITI-72]
Request Verify Token
IUA* Introspect Token [ITI-102]
Return Verify Token Result
Return Resource