8/1/19 – Directory Tiger Team

Alix Goss

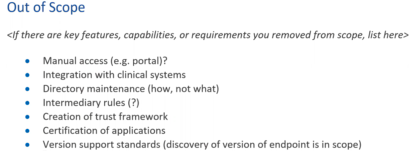
Bob Dieterle

Brandon Neiswender

Rick Geimer

Alex Kontur

Endpoint Discovery Proposed Solution



Out of scope:

* Creation of trust framework & certifying applications (however, recording/presenting participation/certification during endpoint discovery is in scope)
* Out of scope items from use case documentation:
  + Specific architectural requirements (however, high-level architecture/model is in scope)
    - Geimer – We need to be able to explain how it all works together (high-level architecture)
    - Bob – the high-level architecture (model) is in scope but the detail behind the model is not (e.g. the internal architectural design for responding to a query)
    - Geimer – need to provide enough architecture that if you pass it off to a senior architect they would be able to take what we’ve produced, understand intent, and begin building out more detailed architectural requirements
  + Authentication/authorization (considered a “core capability” use case)
    - Brandon – feels like they are components of a high-level architecture
    - Alix – authz/authn are functions that have to happen in a workflow, but the detail about how to perform authz/authn is separate
    - Brandon – we could require something like “standards-based authentication with x components”
    - Bob – in scope as it pertains to endpoint discovery, e.g. discovery of certain types of endpoints may require authorization/authentication. Out of scope as it pertains to the general ecosystem or authenticating/authorizing to a particular service (however, may need to record any such requirements as part of endpoint discovery)
    - Brandon – there will be a way for an organization to discover FHIR-based endpoints/resources from a directory that certifies/records endpoints. Will create an authz/authn construct that allows for an organization/individual to query and understand what FHIR endpoints are available
    - Bob – correct, also saying that it is in scope for the directory to include authn/authz requirements for using a particular endpoint if necessary, e.g. “for this endpoint, you must be authenticated/authorized based on the associated trust framework”. We won’t describe how, just note that you have to do it
  + Internal processing to request endpoints/respond to endpoint requests
    - Alix – anything that feeds nodes from an internal processing perspective is out of scope. A system’s internal dynamics for feeding an endpoint’s request/response processes is out of scope
    - Bob – the operational implementation of it
    - Alex – for example, parsing the query syntax
    - Alix – how an entity processes data requests internally
    - Bob – will have method for requesting an endpoint (including the content/syntax of the request)…how you create the request internally is out of scope as long as the request aligns with the standard. On the other side, we will define the response to the request, but how the response is generated is out of scope
    - Brandon – the response itself and its payload are in scope
    - Alix – the attributes and data elements of the response are in scope
    - Bob – the payload and exchange are in scope, but how it is done internally is out scope
    - Geimer – it’s a black box. You just need to comply with what goes over the wire and the contract that we define
  + Non-FHIR endpoints (if you aren’t using FHIR, we won’t provide the standards)
    - Geimer – however, non-FHIR content sent to FHIR endpoints is in scope (e.g. posting a pdf to the binary endpoint of a FHIR server)
    - Bob – Consider CDS hooks and SMART apps, which are in scope.
    - Geimer – xds or SOAP-based endpoints are out of scope. We are relying on the FHIR API and related stuff like CDS hooks. Technically CDS hooks are not pure FHIR, because they have JSON wrappers that aren’t FHIR resources
    - Brandon – but we’re just talking about endpoint discovery, so it seems like they would be out of scope
    - Geimer – is there any case where we would do CDS hooks? We might do Subscriptions.
    - Brandon – FHIR resources are the basis of the directory, but we don’t care what those resources are
    - Bob – we are talking about endpoints, not the content. The endpoint is for any service that is either a FHIR server or FHIR service. FHIR-related endpoints (e.g. CDS Hooks) as well
    - Geimer – are we going to consider posting FHIR resources to an FTP server? I think not. It wouldn’t use the FHIR API, and can be done out of band
    - Bob – raises an interesting question. Consider bulk data, is it in scope or out of scope if it uses SFTP?
    - Brandon – we aren’t talking about what you can/can’t do. We’re not saying that a directory can’t use an architectural design that allows a user to send an SFTP file to be processed against the API
    - Geimer – if the bulk data spec says you can use SFTP, it’s a FHIR spec and we can just point to it. Won’t say you can’t do it. But we won’t design anything that says you should use SFTP to send a bundle of resources
    - Bob – Let’s say I’m a provider organization that works with a number of payers and I want to get bulk claims data from them on a regular basis. I’m going to use a variant of the FHIR spec in which I publish an endpoint for receiving bulk transfers. The payers extract data on a monthly basis and send it to the endpoint. Is that something that makes sense in the future? I think so
    - Geimer – sounds to me like an agreement between two business partners, not something that we are going to define
    - Bob – but is including that endpoint in the directory something we should support? I don’t see why not
    - Brandon – as long as it meets the FHIR spec
    - Bob – as long as it involves normal RESTful FHIR exchange or a FHIR-related exchange (e.g. CDS hooks or bulk data), then we would expect to support that endpoint
    - Alex – Essentially two conformance statements: (1) a directory solution must make a FHIR endpoint available for accessing directory information (2) All endpoints listed in the directory must be FHIR or FHIR-related
  + Directory is not responsible for knowing endpoint availability
    - Brandon – is this about monitoring SLA language?
    - Bob – e.g. for payers that have endpoints that are only available during certain hours, or not available on the weekend, etc. Saying that the directory is not responsible for knowing the downtime or unavailability of an endpoint
    - Brandon - does the directory impose SLA requirements or availability expectations on entities publishing to the directory?
    - Bob – SLA assumes 24/7 access
    - Alex – Assuming there is a trust framework governing participation in the directory, there may be requirements for publishing endpoint, e.g. the endpoint must meet a minimum threshold of uptime
    - Brandon – not necessarily requirements on the endpoints, rather when you publish an endpoint you also indicate the availability of the endpoint that you wish to hold yourself accountable for
    - Geimer – do we allow entities to say “this endpoint will be down every Sunday for maintenance”
    - Alex – we allow that, but don’t impose a requirement on the directory itself to check
    - Alix – who would have the responsibility for ensuring that kind of attribute is available?
    - Brandon – why does it matter? Nobody will want to use an endpoint that is unavailable/unreliable
    - Alex – the entity operating the directory can impose requirements about what information/content about the endpoint must be published to the directory. The directory may require an endpoint to include general availability. Suggesting that the directory doesn’t have to read that information and check the endpoints on a continuous basis to make sure they are doing what they said they would
    - Geimer – allowing endpoints to attest to their availability, but not verifying their availability
    - Alix – there is a testing/certification component (another Tiger Team), which any requirements will have to align with
    - Alex – as part of our solutioning work, we’ll want to consider all of the possible data elements associated with endpoints that a directory might require entities to publish
    - Bob – monitoring availability is out of scope, support for availability specifications (e.g. SLA, hours of operation) are in scope
  + Alix – a few others to consider: error messages and responses, test vs. production environments, endpoint capabilities, permitted accesses

In scope:

* Bob - Compliance with FHIR (and RESTful) standards for error handling. Assuming that compliance will be part of testing/certification
  + Alix – we are responsible for defining the elements of the certification program, but the line is unclear. Also unclear what the testing/certification Tiger Team is working on
  + Bob – reasonable for the directory to declare whether someone is compliant with FHIR/RESTful standards. Question is whether we use testing/certification or attestation
  + Alex – seems like a more detailed architecture question. We could conceivably create a directory solution using either approach, so specifying one or the other seems unreasonable
  + Bob – are we talking about compliance of the endpoints in the directory, or of the directory itself?
  + Alex – as I am querying the directory, to the extent that it is unavailable or I don’t ask the right question and it creates an error, those errors will be compliant with FHIR and RESTful standards. The actual interactions with the endpoints that I find in the directory are out of scope
  + Bob – do we want an endpoint to declare that it uses standard error responses?
  + Alix – need to be clear about what we expect to establish as standards related to the directory
  + Geimer – our statement that endpoints must be compliant with the FHIR spec cover this. You can’t call it a FHIR endpoint if you don’t have a capability statement, support the REST API, etc. Error handling and using the appropriate HTTP response codes from the FHIR spec are part of that. But we still need to specify that the directory will also be compliant
  + Bob – what if an endpoint offers error response beyond what is required in the FHIR spec?
  + Geimer – as long as they are compliant (e.g. using extensions, OperationOutcome)
  + Alix – directory-level errors and responses are in scope
* Alix – are we assuming that the directory is only a production environment? I would assume there is a test environment
  + Bob – not unreasonable to specify that there is a test environment so people understand they have the ability to test against something
* Alix – use of access tokens?
  + Alex – probably falls under authorization
* Alix – whether the directory permits discovery by anyone…the rules for determining who can access the directory are in scope
  + Brandon – if organizations are going to provide data but require consent or authorization…seems like a feature of the endpoint, not necessarily the directory
  + Alex – talking about discovery of the endpoint itself. If there is an endpoint for a sensitive resource (e.g. a military endpoint), it won’t just be accessible to everybody
  + Alix – in scope for us to define the rules around protecting endpoint discovery
  + Geimer – may be able to push this to the Security Tiger Team?
  + Bob – no, they are focused on security for the endpoints/exchanges, not on access to the directory
  + Alex – isn’t this already covered under authentication/authorization? (Bob – yes)
* Alix – permitted uses (e.g. TPO) which may tie back to a trust framework/agreements. Is there some attribute in the directory that we need to consider? May be covered already?
  + Bob – I think it falls under trust framework
  + Alex – or authorization
* Recording/presenting information about participation in a trust framework and/or application certification
* High-level architecture/model
* Authentication/authorization as it relates to endpoint discovery (e.g. authentication/authorization to ask for information about an endpoint; authentication/authorization requirements for accessing/using an endpoint)
* Payload & exchange
* Test environment for directory

Brandon – how do we envision this playing out across the nation? Do we expect to see organizations that aggregate multiple FHIR endpoints (federated), or there will be a centrally managed directory?

* Bob – one directory that aggregates endpoints with the ability to replicate the data to local directories that provide the information to support workflows. Otherwise you’d have to check each individual directory and/or need a directory of directories