

Inferno Tech Talk – August 2024

Robert Scanlon

MITRE Inferno Team

August 14, 2024

MITRE | SOLVING PROBLEMS
FOR A SAFER WORLD™

Inferno Tech Talk Introduction

- Purpose: to provide regularly scheduled updates on the Inferno tool and its implementation of the (g)(10) test procedure
- Typical agenda to include:
 - Announcements about upcoming releases
 - Training on new features
 - Highlight outstanding issues or known problems
 - Open discussion
- Monthly recurrence: 2nd Wednesday at 1PM ET
- [This call is being recorded and will be posted on https://inferno.healthit.gov/events/](https://inferno.healthit.gov/events/)

Content reflects Inferno's implementation of applicable Test Procedure and does not necessarily reflect ONC policy.

Today's Agenda

- (g)(10) Standardized API Test Kit v6.0.0: HTI-1 Release
 - HTI-1 Updates
 - Additional Updates
- Other Test Kit Updates
- Discussions / Questions

ONC (g)(10) Standardized API Test Kit v6.0.0

- Major release that incorporates all HTI-1 requirements
- Mostly additive to existing test structure
 - Limited changes made to existing tests
 - New scenarios introduced that cover new requirements
- Many tests have been previously released in other Test Kits (e.g. US Core Test Kit & SMART App Launch Test Kit) or as optional SVAP standards in (g)(10) Test Kit
- Inferno Reference Server updated and pass all tests; Walkthrough update in process
- Release also includes a few updates outside the scope of HTI-1

Available for Download

<https://github.com/onc-healthit/onc-certification-g10-test-kit/releases/tag/v6.0.0>

ONC Hosted Instance

<https://inferno.healthit.gov/test-kits/g10-certification/>

Summary of Updates

▪ HTI-1 Specific Updates

- Add checks for additional SMART capabilities ([#534](#)).
- Add Token Introspection tests ([#531](#)).
- Add Asymmetric Client Auth tests ([#533](#)).
- Add SMART App Launch v1 scopes tests ([#535](#)).
- Add SMART Granular Scopes tests ([#537](#)).
- Add tests for the selection of granular scopes when resource-level scopes are requested ([#539](#)).
- Add an attestation for supporting the Observation Clinical Test granular scope ([#543](#)).
- Moves the Visual Inspection and Attestation tests to their own top-level group ([#540](#)).

▪ Other Fixes/Updates

- Add US Core 6 Screening and Assessment test group ([#542](#)).
- Fix an issue which only used the code value and ignored the system when checking for the presence of Must Support slices based on bound Value Sets ([#536](#)).

HTI-1 specific (g)(10) Test Kit Updates

HTI-1 Final Rule Resources

- **ONC Informational Material:**
 - <https://www.healthit.gov/topic/laws-regulation-and-policy/health-data-technology-and-interoperability-certification-program>
- **HTI-1 Final Rule:**
 - <https://www.federalregister.gov/documents/2024/01/09/2023-28857/health-data-technology-and-interoperability-certification-program-updates-algorithm-transparency-and>
- **(g)(10) Certification Companion Guide & Test Procedure:**
 - <https://www.healthit.gov/test-method/standardized-api-patient-and-population-services>

Most of the new tests apply to the new baseline versions of standards set by HTI-1.

Older versions of standards still available for certification until phased out as described in HTI-1

Start Testing

US Core Version

- US Core 3.1.1 / USCDI v1
- US Core 4.0.0 / USCDI v1
- US Core 6.1.0 / USCDI v3

SMART App Launch Version

- SMART App Launch 1.0.0
- SMART App Launch 2.0.0

Bulk Data Version

- Bulk Data 1.0.1
- Bulk Data 2.0.0

[+ Create Test Session](#)

Updates are isolated* in additional tests when selecting latest approved versions of standards

* One exception: SMART well-known capabilities check in early scenarios was updated

Also note that “Visual Inspection” was moved to its own top-level group, and “Additional Tests” group was renamed to “Additional Authorization Tests”

- (g)(10) Standardized API
 - 1 Standalone Patient App
 - 2 Limited Access App
 - 3 EHR Practitioner App
 - 10 Single Patient API
 - 8 Multi-Patient API STU2
 - ▼ 9 Additional Authorization Tests
 - 9.2 Public Client Launch
 - 9.3 Token Revocation
 - 9.4 Invalid AUD Launch
 - 9.6 Invalid Token Request
 - 9.7 Invalid PKCE Code Verifier
 - 9.9 EHR Launch with Patient Scopes
 - 9.11 Token Introspection
 - 9.12 Asymmetric Client Launch
 - 9.13 Launch with v1 Scopes
 - ▼ 9.14 SMART Launch with Fine-Grained Scopes
 - 9.14.1 Granular Scopes 1
 - 9.14.2 Granular Scopes 2
 - 9.15 SMART Granular Scope Selection
 - 11 Visual Inspection

Unchanged from previous release *

New Tests

Additional SMART Capabilities Discovery check

Presets: None

(g)(10) Standardized API

- 1 Standalone Patient App
- 2 Limited Access App
- 3 EHR Practitioner App
- 10 Single Patient API
- 8 Multi-Patient API STU2
- 9 Additional Authorization Tests
 - 9.2 Public Client Launch
 - 9.3 Token Revocation
 - 9.4 Invalid AUD Launch
 - 9.6 Invalid Token Request
 - 9.7 Invalid PKCE Code Verifier
 - 9.9 EHR Launch with Patient Scopes
 - 9.11 Token Introspection
 - 9.12 Asymmetric Client Launch
 - 9.13 Launch with v1 Scopes
 - 9.14 SMART Launch with Fine-Grained Scopes
 - 9.14.1 Granular Scopes
 - 9.14.2 Granular Scopes

access token to ensure that the refresh was successful. The authentication information provided by OpenID Connect is decoded and validated, and simple queries are performed to ensure that access is granted to all USCDI data elements.

Prior to running the scenario, register Inferno as a confidential client with the following information:

- Redirect URI: <https://inferno.healthit.gov/suites/custom/smart/redirect>

The following implementation specifications are relevant to this scenario:

- [SMART on FHIR \(STU1\)](#)
- [SMART on FHIR \(STU2\)](#)
- [OpenID Connect \(OIDC\)](#)

1.2 SMART on FHIR Discovery

About SMART on FHIR Discovery

- 1.2.01 FHIR server makes SMART configuration available from well-known endpoint
- 1.2.02 Well-known configuration contains required fields
- 1.2.03 Well-known configuration declares support for required capabilities

1.4 Standalone Launch With Patient Scope

1.5 OpenID Connect



HTI-1 requires implementation of the 'client-confidential-asymmetric' capability in SMART App Launch v2, and to support the 'permission-v1' for backwards compatibility

```
lib/onc_certification_g10_test_kit/smart_standalone_patient_app_group.rb
```

@@ -93,12 +93,14 @@ class SmartStandalonePatientAppGroup < Inferno::TestGroup	
93 'launch-standalone',	93 'launch-standalone',
94 'client-public',	94 'client-public',
95 'client-confidential-symmetric',	95 'client-confidential-symmetric',
	96 + 'client-confidential-asymmetric',
96 'sso-openid-connect',	97 'sso-openid-connect',
97 'context-standalone-patient',	98 'context-standalone-patient',
98 'permission-offline',	99 'permission-offline',
99 'permission-patient',	100 'permission-patient',
100 'authorize-post',	101 'authorize-post',
101 - 'permission-v2'	102 + 'permission-v2',
	103 + 'permission-v1'
102]	104]
103 }	105 + }
104 }	106 }

Token Introspection (1/2)

- HTI-1 requires a standard API implementation for Token Introspection (previously only a functional requirement)
- Specification provided by SMART App Launch v2.0.0
- Incorporates Token Introspection tests from the SMART App Launch Test Kit that were initially released in December 2023
- Requires demonstration of introspecting an active bearer token and a known invalid token
- Token introspection preceded by a SMART App Launch to retrieve a new bearer token

9.11 Token Introspection

[▶ RUN TESTS](#)

This scenario verifies the ability of an authorization server to perform token introspection in accordance with the [SMART App Launch STU2 Implementation Guide Section on Token Introspection](#). Inferno first acts as a registered SMART App Launch client to request and receive a valid access token, and then as an authorized resource server that queries the authorization server for information about this access token.

The system under test must perform the following in order to pass this scenario:

- Issue a new bearer token to Inferno acting as a registered SMART App Launch client. The tester has flexibility in deciding what type of SMART App Launch client is used (e.g. public or confidential). This is redundant to tests earlier in this test suite, but is performed to ensure an active token can be introspected.
- Respond to a token introspection request from Inferno acting as a resource server for both valid and invalid tokens. Systems have flexibility in how access control for this service is implemented. To account for this flexibility, the tester has the ability to add an Authorization Header to the request (provided out-of-band of these tests), as well as additional Introspect parameters, as allowed by the specification.

9.11.1 Request New Access Token to Introspect ▼

9.11.2 Issue Token Introspection Request ▼

9.11.3 Validate Token Introspection Response ▼

Token Introspection (2/2)

- Access Control method for use of this API is not specified
- Inferno provides flexibility in how this might occur by allowing testers to add ad-hoc headers to the request (e.g. a Bearer token in an Authorization header) that are created out-of-band
- Also allows any arbitrary extra parameters to be added to the introspection request as allowed by the standard
- Please let us know if this needs to be made more flexible

Token Introspection



Token Introspection Endpoint

The complete URL of the token introspection endpoint. This will be populated automatically if included in the server's discovery endpoint.

HTTP Authorization Header for Introspection Request

Include header name, auth scheme, and auth parameters. Ex:
'Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW'

Additional Introspection Request Parameters

Any additional parameters to append to the request body, separated by &. Example: 'param1=abc¶m2=def'

Asymmetric Client Authentication for SMART Launch

- HTI-1 requires support for the **client-confidential-asymmetric** capability for patient/user scopes
- Instead of adjusting existing launches, we add a separate launch
- Inferno JWKs URL provided in the input instructions when running tests; functions similar to the Multi-Patient API authorization

The screenshot displays the Inferno test suite configuration interface. On the left, a list of tests is shown with radio buttons for selection. The test '9.12 Asymmetric Client Launch' is highlighted. On the right, the details for the selected test are shown, including a description of the 'Standalone Launch Sequence' and a list of sub-tests: '9.12.1 SMART on FHIR Discovery', '9.12.2 SMART Standalone Launch', and '9.12.3 Token Refresh'. A 'RUN TESTS' button is visible in the top right corner of the details panel.

Preset: None

- 10 Single Patient API
- 8 Multi-Patient API STU2
- 9 Additional Authorization Tests
 - 9.2 Public Client Launch
 - 9.3 Token Revocation
 - 9.4 Invalid AUD Launch
 - 9.6 Invalid Token Request
 - 9.7 Invalid PKCE Code Verifier
 - 9.9 EHR Launch with Patient Scopes
 - 9.11 Token Introspection
 - 9.12 Asymmetric Client Launch
 - 9.13 Launch with v1 Scopes
 - 9.14 SMART Launch with Fine-Grained Scopes
 - 9.14.1 Granular Scopes 1
 - 9.14.2 Granular Scopes 2
 - 9.15 SMART Granular Scope Selection
- 11 Visual Inspection

9.12 Asymmetric Client Standalone Launch RUN TESTS

The [Standalone Launch Sequence](#) allows an app, like Inferno, to be launched independent of an existing EHR session. It is one of the two launch methods described in the SMART App Launch Framework alongside EHR Launch. The app will request authorization for the provided scope from the authorization endpoint, ultimately receiving an authorization token which can be used to gain access to resources on the FHIR server.

These tests specifically verify a system's support for [confidential asymmetric client authentication](#), which is not verified in earlier scenarios.

In this scenario, Inferno will redirect the user to the the authorization endpoint so that they may provide any required credentials and authorize the application. Upon successful authorization, Inferno will exchange the authorization code provided for an access token.

For more information on the Asymmetric Client Standalone Launch:

- [Standalone Launch Sequence](#)

- 9.12.1 SMART on FHIR Discovery
- 9.12.2 SMART Standalone Launch
- 9.12.3 Token Refresh

Launch with v1 Scopes

- Existing (g)(10) SMART v2 tests only verified use of SMART v2-style scopes
- ONC requires support for SMART v1 as well, for clients that may not support SMART v2 style scopes
- Additional test performs another launch that request SMART v1 scopes, and ensures that a Bearer token is granted that allows access to all relevant USCDI resource types
 - Not opinionated about what form of scopes are granted
- Inferno may be registered with a separate `client_id` if necessary

The screenshot shows a web-based test configuration interface. On the left is a sidebar with a 'Preset' dropdown set to 'None' and a list of test categories with radio buttons. The selected category is '9.13 Launch with v1 Scopes'. The main panel displays the details for '9.13 App Launch with SMART v1 scopes', including a 'RUN TESTS' button, a description of the scenario, and a list of sub-scenarios.

9.13 App Launch with SMART v1 scopes RUN TESTS

This scenario verifies the ability of a system to support a Standalone Launch when v1 scopes are requested by the client. It verifies that systems implement the `permission-v1` capability as required. Previous scenarios focus on the use of the `permission-v2` capability, and thus a dedicated launch is required to verify that systems can support a client that requests `permission-v1` style scopes.

This scenario does not place any constraints on the form of scopes granted. Systems are free to grant v1-style scopes in response to the request for v1-style scopes, as recommended in the [SMART App Launch Guide STU2](#). Or they can upgrade them to v2-style scopes. The scenario only ensures that systems can grant access to clients that request v1-style scopes and that the client has access to resources as expected.

All relevant resource types must be granted, in a similar manner to the 'Standalone Patient App' scenario.

This scenario expects Inferno to be registered as a 'Confidential Symmetric' client. Systems may either reuse a `client_id` associated with Inferno used in a previous scenario, or register Inferno with a new `client_id` as a standalone client with the following information:

- Redirect URI: `https://inferno.healthit.gov/suites/custom/smart/redirect`

9.13.1 SMART on FHIR Discovery

9.13.2 Standalone Launch With Patient Scope

9.13.3 Unrestricted Resource Type Access

SMART Launch with Fine-Grained Scopes (1/2)

- Verifies ability of a system to support “Granular Scopes” or “Fine-grained Scopes” as described in SMART App Launch v2
- Based on tests introduced in February into the US Core Test Kit and demonstrated for feedback from the community
- ONC specifically requires support for: (1) the Condition resource with Condition sub-resources Encounter Diagnosis, Problem List, and Health Concern and (2) the Observation resource with Observation sub-resources Clinical Test, Laboratory, Social History, SDOH, Survey, and Vital Signs.
- Specific scopes used in tests defined by US Core
- Clinical Test Observation is ambiguous and requires an attestation

SMART Launch with Fine-Grained Scopes (2/2)

- Prior to running this test, systems must first run the ‘Single Patient API’ tests which gather all available information relating to a patient or set of patients
- This test performs two extra launches, each with a subset of finer-grained scopes to be granted
- After each bearer token is granted, the tests perform the same set of searches as the Single Patient API and verifies that appropriate resources can be accessed with limited scope

The screenshot displays the ONC Certification (g)(10) Standardized API v.6.0.0 interface. The main title is "ONC Certification (g)(10) Standardized API v.6.0.0" with a "NEW SESSION" button. Below the title, it specifies "US Core 6.1.0 / USCDI v3, SMART App Launch 2.0.0, Bulk Data 2.0.0".

The interface is divided into two main sections:

- Left Panel (Preset):** A dropdown menu is set to "None". Below it is a list of test categories with radio buttons:
 - 9.6 Invalid Token Request
 - 9.7 Invalid PKCE Code Verifier
 - 9.9 EHR Launch with Patient Scopes
 - 9.11 Token Introspection
 - 9.12 Asymmetric Client Launch
 - 9.13 Launch with v1 Scopes
 - 9.14 SMART Launch with Fine-Grained Scopes (expanded)
 - 9.14.1 Granular Scopes 1
 - 9.14.2 Granular Scopes 2** (highlighted)
 - 9.15 SMART Granular Scope Selection
 - 11 Visual Inspection
- Right Panel (9.14.2 Granular Scopes 2):** A "RUN TESTS" button is visible. The main content area contains:
 - A green checkmark icon and the title "9.14.2 Granular Scopes 2".
 - A description: "These tests perform a SMART app launch to receive the following granular scopes:"
 - A bulleted list of scopes:
 - Condition.rs?category=http://terminology.hl7.org/CodeSystem/condition-category|problem-list-item
 - Observation.rs?category=http://terminology.hl7.org/CodeSystem/observation-category|vital-signs
 - Observation.rs?category=http://terminology.hl7.org/CodeSystem/observation-category|survey
 - Observation.rs?category=http://hl7.org/fhir/us/core/CodeSystem/us-core-category|sdo
 - A note: "Then all of the searches which have been performed in the US Core FHIR API tests are repeated to verify that the results have been filtered according to the above scopes."
 - A list of sub-tests:
 - 9.14.2.1 Standalone Launch
 - 9.14.2.2 Condition Granular Scope Tests Tests
 - An expandable section titled "About Condition Granular Scope Tests Tests" with a dropdown arrow.
 - Sub-test details for "9.14.2.2.01 Server filters results for Condition search by patient + category based on granular scopes" with a green checkmark and a "9+" icon.

SMART Granular Scope Selection (1/3)

- ONC provided the following clarification in the CCG:

As part of supporting the SMART App Launch “permission-v2” capability for the purposes of certification, if an app requests authorization for a resource level scope for the “Condition” or “Observation” resources, then for patient authorization purposes a Health IT Module must support presentation of the required sub-resource scopes to the patient for authorization. Specifically, sub-resource scopes must be presented for patient authorization as follows:

- “Condition” sub-resource scopes “Encounter Diagnosis”, “Problem List”, and “Health Concern” if a “Condition” resource level scope is requested
- “Observation” sub-resource scopes “Clinical Test”, “Laboratory”, “Social History”, “SDOH”, “Survey”, and “Vital Signs” if an “Observation” resource level scope is requested

SMART Granular Scope Selection (2/3)

- This test verifies that when resource-level scopes are REQUESTED, the patient user can choose to instead GRANT sub-resource-level scopes
- In some ways, this is similar to the 'Limited Access App' tests in that it is verifying the ability of the patient user to authorize something different than what an app requests
- However, this is not just a subset of requested scopes; they are different scopes that are a logical subset
- The test performs a launch and instructs the tester to not grant access to the requested Condition and Observation scopes, but instead grant only those

SMART Granular Scope Selection (3/3)

- Example scope selection screen from the Inferno Reference Server (implementations do NOT have to look like this, this is just an example that enables the required functionality):

Inferno ONC Standardized API Demo Server

Please select which scopes you would like to authorize. To select a granular resource scope, first de-select the full resource scope.

- launch/patient
- openid
- fhirUser
- offline_access
- patient/Condition.rs
 - patient/Condition.rs?category=http://hl7.org/fhir/us/core/CodeSystem/condition-category|health-concern
 - patient/Condition.rs?category=http://terminology.hl7.org/CodeSystem/condition-category|encounter-diagnosis
 - patient/Condition.rs?category=http://terminology.hl7.org/CodeSystem/condition-category|problem-list-item
- patient/Observation.rs
 - patient/Observation.rs?category=http://hl7.org/fhir/us/core/CodeSystem/us-core-category|sdoh
 - patient/Observation.rs?category=http://terminology.hl7.org/CodeSystem/observation-category|social-history
 - patient/Observation.rs?category=http://terminology.hl7.org/CodeSystem/observation-category|laboratory
 - patient/Observation.rs?category=http://terminology.hl7.org/CodeSystem/observation-category|survey
 - patient/Observation.rs?category=http://terminology.hl7.org/CodeSystem/observation-category|vital-signs
- patient/Patient.rs

Clinical Test Observation Scope

- There's no clear mapping from Clinical Test to a specific category code
- Rather than an automated test for a specific category code, we have the user attest that the system supports granting a sub resource scope for Clinical Test Observations

Visual Inspection and Attestation ×

Health IT developer attested that the Health IT Module meets the requirements for supporting the `_since` parameter for bulk data exports. (required) *

Yes No

Notes, if applicable:

Health IT developer attested that the Health IT Module supports granting a sub resource scope for Clinical Test Observations. (required) *

Yes No

Notes, if applicable:

FIELD JSON YAML CANCEL **SUBMIT**

Additional (g)(10) Test Kit Updates

Observation Screening and Assessment Patch

ONC CCG

Applies to US Core 6.1.0 and USCDI v3 (required by December 31, 2025):

- The HL7[®] Cross-Group Projects workgroup approved the [US Core 'Patch' Process](#) ticket [FHIR-45319](#) for US Core 6.1.0. In alignment with that issued guidance, the Health IT Module must support all four codes from the US Core Screening Assessment Observation Category ValueSet for the US Core Observation Screening Assessment Profile for “Observation.category:screening-assessment”. Additionally, the Health IT Module must support the “sdoh” code from the US Core Screening Assessment Condition Category ValueSet for the US Core Condition Problems and Health Concerns Profile for “Condition.category:screening-assessment”.

10.47 Screening Assessments Guidance

About Screening Assessments Guidance

The Screening Assessments Guidance Sequence tests Condition and Observation resources associated with the provided patient. The resources returned will be checked for consistency against the [US Core Screening And Assessments Guidance](#) and FHIR JIRA ticket [FHIR-45319](#)

In this set of tests, Inferno serves as a FHIR client that attempts to access the different types of Screening and Assessments specified in the guidance. The provided patient needs to have the following four common Screening and Assessments as Observation categories:

- SDOH Assessment (sdoh)
- Functional Status (functional-status)
- Disability Status (disability-status)
- Mental/Cognitive Status (cognitive-status)

The provided patient also needs to have the following common Screening and Assessment as Condition category:

- SDOH Assessment (sdoh)

MustSupport test on requiredBinding slices

We found that Inferno US Core MustSupport test on requiredBinding slicing only verifies coding.code.

One example is on Observation.category

Observation SDOH Assessment profile in US Core 5 has slice with requiredBinding <http://hl7.org/fhir/us/core/CodeSystem/us-core-tags|sdoh>.

Observation Screening and Assessment profile in US Core 6 has slice with requiredBinding <http://hl7.org/fhir/us/core/CodeSystem/us-core-category|sdoh>.

Without coding.system value, MustSupport test could incorrectly pass MustSupport test using Observations instance with incorrect sdoh coding.

Other Test Kit Releases

- Introducing UDAP Security Test Kit (v0.9)
 - <https://inferno.healthit.gov/test-kits/udap-security/>
 - Replaces the FAST Security Test Kit
 - Aligned to requirements in the [Security for Scalable Registration, Authentication, and Authorization IG](#)
- Incremental updates to the following Test Kits:
 - US Core Test Kit v0.8.0
 - Da Vinci Payer Data Exchange (PDex) Test Kit v0.10.5
 - Da Vinci Prior Authorization Support (PAS) Test Kit v0.10.1
 - Service Base URL Test Kit v0.10.1
 - SMART App Launch Test Kit v0.4.3e

Open Discussion / Feedback

Resources and Contact Information

- <https://inferno.healthit.gov/>
 - General materials & live demonstration server
- <https://inferno-framework.github.io>
 - Create your own Inferno Test Kits!
- <https://github.com/onc-healthit/onc-certification-g10-test-kit/>
 - ONC Certification tests repository, downloads, issues
 - “Watch” repository to receive alerts (new releases, etc)
 - Note: this repository is specific to ONC Certification testing
- inferno@groups.mitre.org (or rscanlon@mitre.org)
- FHIR Zulip Chat: <https://chat.fhir.org/#narrow/stream/179309-inferno>

Upcoming Meetings

- Next Inferno Tech Talk: **Wednesday September 11** at 1 PM ET
- Please reach out with questions & issues