Access 4 Learning Community

Powered by: SIF

Simple. Secure. Scalable. Standard.

SIF 3 Product Standard

www.A4L.org

Issue 1 v5, May 2017

NAME **SIF 3 Product Standard**

LABEL FOR LOGO **SIF 3 + Infrastructure, Locale Name, or Profile Name, such as *SIF 3 (North America)***

PURPOSE To create a policy framework document outlining the particular implementation details and requirements for SIF Certification.

DESCRIPTION The SIF 3 Product Standard defines the requirements for an application to be considered conformant to the SIF Implementation Specification (see below). The following definitions are used in this document:

- The SIF Implementation Specification is one of any of the releases of the SIF Implementation Specification in the 3 major release cycle for which a sanctioned test suite is provided for use in certification, supplemented by any Interpretations[1] (in this document or the errata to the specification) applicable to this particular version and revision of the Specification. For a description of Interpretations, see Section 9.3.1 of the SIF Certification Program Policy.
- A Certified Application is a product or service that has successfully completed the certification process and for which the Solution Provider has been notified in writing by the Certification Authority that certification has been achieved for such product or service. The details of these requirements are disclosed throughout the SIF Implementation Specification[2].
- An Environment Provider manages Certified Applications from the simplest service to the core of a logical enterprise setting. See Appendix B of the SIF Infrastructure Services document for a summary of the types and roles of Environment Providers.
- The Transport Layer Security (TSL) is version 1.1 of the TSL protocol, as specified in IETF RFC 4346[3]. For a discussion of TLS backward compatibility when negotiating connection parameters, see Appendix E of IETF RFC 4346. TLS details used for certification can be found in the Security Requirements section of this document. This section incorporates (and refines) requirements found in the SIF 3 Base Architecture document.

[1] *https://a4l.site-ym.com/resource/collection/D44B484D-4C49-4A46-BC51-FB1D3F672D15/SIF%20Certification%20Program%20Policy.pdf*
[2] *SIF Implementation Specification documentation: https://a4l.site-ym.com/page/SIFSpecifications*
[3] *IETF RFC 4346: http://www.ietf.org/rfc/rfc4346.txt*

- HTTP is version 1.1 of the Hypertext Transport Protocol, as specified in IETF RFC 2616[4]
- XML is version 1.0, Third Edition, of the Extensible Markup Language, as specified in the W3C Recommendation of February 4, 2004.
- UTF-8 is a data encoding process refined by IETF RFC 2279[5] of ISO 10646.
- REST is the building of services directly upon HTTP. The SIF Infrastructure specifies URL and HTTP Header requirements in a RESTful style. For tables detailing the use of these structures see Appendix C of the SIF Infrastructure Services document.
- XPath 2.0[6] is a W3C recommended expression language for working with XML documents.
- XQuery 1.0[7] is an XML query language recommendation published by the W3C.
- The SIF Specifications define XML Schemas (XSDs) for payload exchanged between an Environment Provider and a Certified Application. These files are downloadable from the Access 4 Learning (A4L) Community's public website[8].
- Gzip is a compression scheme that may be employed to reduce the size of payloads.

A GUID is a Globally Unique Identifier (also known as a UUID or Universally Unique Identifier), is widely utilized in both the SIF Infrastructure and Data Model as specified in the IETF RFC 4122[9].

SECURITY REQUIREMENTS

The SIF 3 Product Standard, in order to ensure interoperability with both the Test Harness and other Certified Applications and services, includes the following requirements around security:

- All supported authentication schemes are treated as optional, however at least one must be chosen.

[4] *IETF RFC 2616: http://www.ietf.org/rfc/rfc6266.txt*
[5] *IETF RFC 2279: http://www.ietf.org/rfc/rfc2279.txt*
[6] *XPath 2.0: http://en.wikipedia.org/wiki/XPath_2.0*
[7] *XQuery 1.0: http://en.wikipedia.org/wiki/XQuery*
[8] *All SIF Specifications can be found on the A4L website here: https://a4l.site-ym.com/page/SIFSpecifications*
[9] *IETF RFC 1422: http://www.ietf.org/rfc/rfc4122.txt*

- When leveraging OAuth 2.0/Bearer authentication any supplied Initial Session Token is used as the client_id and any supplied Consumer Secret is used as the client_secret.
- Certificates exchanged to verify identity employ a key length of at least 2048bits.
- All certificates employed must be current.
- All valid certificates will be accepted.
- Hostname and certificate mismatches are allowed.
- All encrypted connections employ a cypher with a minimum key length of 128bits.
- TLS handshakes must be done in SSL 3.0 style and support the TLS 1.1 version {3, 2} within.
- Connections must support TLS 1.1.

COMPATIBILITY REQUIREMENTS

Interoperability between versions of SIF Specifications utilized in products is critical to on-going technology support. Because of this, SIF Certified Products are held to these resulting necessities.

- Certified Products must work with existing applications utilizing the same SIF (infrastructure and data model) versions and those only varying by the revision number.
- Certified Products must function without change with applications written to new versions of SIF that only differ by the revision number.

CONFORMANCE REQUIREMENTS

The conformance requirements of the SIF 3 Product Standard for a Certified Application are derived from the SIF Specification. A Certified Application must demonstrate that it can:

- Create an Environment with the Environment Provider and/or create an Access Token as defined by a profile.
- Provide or Request/Subscribe and Receive data objects via the Environment Provider as disclosed in the application's CSQ.
- Encrypt, transport, and authenticate SIF messages in a manner that conforms to the Security Requirements section of this document.
- Exchange messages that are uniquely identified by a GUID and sequenced and processed in a manner that conforms to the SIF 3 Infrastructure.

- Produce messages that conform to the data definitions of the SIF Infrastructure version referenced by the Test Suite. Required and mandatory elements must be supported; and optional and conditional elements may be supported at the discretion of the implementer, as indicated in the CSQ.
- Produce messages containing data objects that conform to the SIF Data Model in the version referenced by the Test Suite. Required and mandatory elements must be supported; optional and conditional elements may be supported at the discretion of the implementer.
- Receive/process messages that conform to any SIF Infrastructure version in the 3 major release cycle (this requirement may be met by responding with the appropriate error).
- Receive/process messages containing data objects that conform to the data definitions of the SIF Message Specification in any SIF Implementation Specification version in the 3 major release cycle (this requirement may be met by responding with the proper error).
- Similar support for objects claimed in relation to a service path[10] must also be demonstrated using object services[11].
- Providers may be required to demonstrate JSON[12] support (in addition to XML) based on the release or profile the Test Suite is built for.

There are no requirements placed upon a Certified Application that constrain the way that the conformance requirements are met, and in particular there are no requirements concerning how any software components are integrated together to constitute a conforming product or service.

INDICATORS OF CONFORMANCE

A test report from a currently approved formal release of the SIF 3 Application Test Suite is required. The Test Suites will be hosted on the Access 4 Learning (A4L) Community's web server and accessed over the Internet.

[10] *See the glossary of terms: service path.*
[11] *See the glossary of terms: object services.*
[12] *See the glossary of terms: JSON.*

PREVIOUS SPECIFICATION VERSIONS

A major release version occurs when you make significant specification changes characterized by the SIF 3 Implementation Specification for the marketplace. A significant change can be defined as one of the following:-

a. Deprecating payload representation.

b. Removing deprecated payload representation.

c. Adding support for a new data model namespaces.

d. Replace (deprecate and remove) a locale data model.

e. Any significant change that requires the major version to be incremented as deemed by the A4L Community Board for global specifications and Management Boards for locale data models.

Revision History:

Issue	Date	Change History
V0	June 2014	First release of the SIF 3 Product Standard.
V1	June 2014	Comparison edits from the original draft and the 2.x draft (LF editor)
V2	July 2014	Final edits from the original draft and the 2.x draft (LF editor)
V3	July 2014	Edited in turns and discussed, considered Final Draft ahead of initial release (RR, JL, & PM editors)
V4	August 2015	Updated to reflect re-brand to the Access 4 Learning (A4L) Community, formerly the SIF Association. (PM editor)
V5	May 2017	Updated to reflect areas of testing added to support xPress Roster.

