

UI SIDES

Separation Information Data Exchange System

Supplemental Specification

Separation Information Data Exchange System (SIDES)

REQUIREMENTS BASELINE

24 December 2008

Copyright © 2008, National Association of State Workforce Agencies.

All Rights Reserved.

Revision History

Date	Version	Description	Author
12/13/2006	DRAFT 1.0	Updated to meeting requests	Lou Ansaldi (ITSC), Jason Holzbach
03/18/2008	DRAFT 2.0	Updated to new architecture	Lou Ansaldi (ITSC), Jason Holzbach
03/24/2008	DRAFT 3.0	Updated following internal review	Lou Ansaldi (ITSC), Jason Holzbach
03/28/2008	DRAFT 4.0	Updated following Consortium Review	Lou Ansaldi (ITSC), Jason Holzbach
03/31/2008	DRAFT 10.0 'Requirements Review Draft'	Marked each requirement that affects the Endpoint(s) requirements Bumped version number to Version 10, to bring all documents to same version number for 4/3/08 requirements review	David Zemel (ITSC), Colin Lennox (ITSC), Jason Holzbach
04/07/2008	Draft 11.0	Updated after Consortium Review Added 2.2.13 Updated 2.3.7	David Zemel (ITSC), Colin Lennox (ITSC), Jason Holzbach
04/09/08	Draft 13.0	Updated after Consortium Review – Changed wording on 2.1.13 Updated version number to Version 13 for Final Review Draft	David Zemel (ITSC), Colin Lennox (ITSC), Jason Holzbach
4/14/08	Draft 14.0	Updated after Consortium review Replaced Routing Table with Connector Table to be consistent with current language REQUIREMENTS BASELINE ISSUE	David Zemel (ITSC), Colin Lennox (ITSC), Jason Holzbach
5/6/08	Draft 15.0	SIGNED OFF VERSION	Lou Ansaldi (ITSC), Jason Holzbach
7/3/08	Draft 16.0	Updated version number to Version 16 for updated Requirements Baseline reflecting approved	Lou Ansaldi (ITSC), Jason Holzbach

Version 18 – Requirements Baseline – 12-24-2008

		<p>changes from CCB #1 document.</p> <p>Changes included in this document are:</p> <p>Requirement 2.1.13 During the design phase, it was recognized that a user may only have one role associated with it. This is due in part to the fact that there are only two roles and the more restrictive role is incorporated in the administrative role.</p> <p>Requirement 2.1.10 During both the design and requirements phase, there was confusion using the work “session” when speaking about the handshake messaging. Therefore, we replaced “session” with “http request/response” which is a more accurate term and the term we used throughout the Design Document.</p>	
7/24/08	17	<p>No Changes</p> <p>Updated version number to Version 17 for updated Requirements Baseline reflecting approved changes from CCB #2 document.</p>	Lou Ansaldi (ITSC), Jason Holzbach
12/24/08	18	<p>No Changes</p> <p>Updated version number to Version 18 for updated Requirements Baseline reflecting approved changes from CCB #3 document.</p>	Lou Ansaldi (ITSC), Jason Holzbach

Table of Contents

2	Supplemental Requirements	5
2.1	Security	5
2.2	Performance and Availability	7
2.3	Design Guidelines	8
2.4	Testing Guidelines	9
2.5	Usability	11
2.6	Data Transactions	12
2.7	Online Help	12
2.8	Accessibility	12
2.9	Metrics	13
2.10	Logging Data	13

2 Supplemental Requirements

2.1 Security

- 2.1.1 The Security model shall document Identification, Authentication, and Authorization in the technical architecture and design document.
- 2.1.2 The Vendor must adhere to the WS-Security specification, with any deviations noted, and justified for approval by the UI SIDES Consortium.
- 2.1.3 The SIDES States consortium requires the Vendor to address how they will specifically provide Transport-level security and Authentication in the technical architecture and design document.
- 2.1.4 Custom tokens via Websphere 6.0 extensions are prohibited.
- 2.1.5 The Vendor security framework and design will consider Capacity, Performance, Roles and Disaster Recovery. This shall be addressed as part of the proposed solution.
- ~~2.1.6 The Broker application security officer (Broker Administrator) must have the ability to execute all Web Service calls.
See requirement 2.1.9~~
- ~~2.1.7 The Broker Administrator must have the ability to execute all web application functions.
See requirement 2.1.9~~
- ~~2.1.8 The Broker Administrator must have the ability to reset external client passwords.
See requirement 2.1.9~~
- 2.1.9 All the capabilities of a user are defined in the Roles Matrix.
- 2.1.10 The Broker web site must provide the ability for an Employer/TPA and/or State to have access to their own data: metrics, query capability per functionality specified in the Use Cases, and the active date associated with their own URI
- 2.1.11 The Broker must provide a user ID that is additionally linked to the user's organization.
- 2.1.12 The Broker must support confidentiality by providing states and employers/TPAs access only to their own accounts (between the connector information and their data). This is supported by Rules and Requirements 123 and 124).
- 2.1.13 The Broker web site shall support two or more concurrent users per participating entity. Each user may have one ~~any (or multiple)~~ role as defined in the roles matrix. [Affects Endpoint(s) Requirements]
- 2.1.14 The Broker must limit access to information according to role.
- 2.1.15 The Broker must validate user identity regarding data access as defined in the Roles Matrix.
- 2.1.16 The system shall encrypt all data at the transport level using HTTPS between itself and endpoints. [Affects Endpoint(s) Requirements]
- 2.1.17 The Broker web service shall be designed to push files to the intended target

- 2.1.18 The Broker shall require HTTPS for State and Employer/TPA login and access.
- 2.1.19 The Broker web site must allow the Employers/ TPAs and States the ability to change their password via a challenge/response mechanism.
- 2.1.20 The password shall conform to the password standards outlined in the Rules and Requirements document.
- 2.1.21 The Broker web site shall allow designated administrators to change user passwords. The new password shall be assigned as temporary.
- 2.1.22 When a user has a temporary password assigned, the Broker web site must force a password change immediately after authentication.
- 2.1.23 The Broker web site shall not display the password in a readable format on the screen when it is being entered.
- 2.1.24 ~~The system shall store the passwords in a place that cannot be found by unauthorized users in a form that is unreadable.~~
Duplicate of 2.1.25
- 2.1.25 The Broker shall require that all passwords be stored with one-way encryption to prevent anyone (including the System Administrator) from reading them.
- 2.1.26 The system must provide secure transport of attachments.
- 2.1.27 The system must create a security audit log record.
- 2.1.28 The Broker shall contain Role Based Access Control (RBAC) features
- 2.1.29 The Broker web site shall provide searching for username/ID, last name
- 2.1.30 The Broker web site shall list users by role to the Administrators.
- 2.1.31 The Broker shall enable establishing and maintaining authorizations and permissions for all users according to role.
- 2.1.32 The Broker web site shall enable an Administrator to set a given role to limit access to specified data
- 2.1.33 ~~The system shall enable an Administrator to set authorization / permission to limit access to specified files, folders and documents.~~
Not Applicable
- 2.1.34 The Broker web site shall enable an Administrator to limit access to specified applications as per the Roles Matrix.
- 2.1.35 Users shall only have to log-on once to gain access to the system functionality they have permission to access as defined in the Roles Matrix.
- 2.1.36 The Broker web site shall log-off a user automatically after 30 minutes of no activity.
- 2.1.37 ~~The system shall provide a way for Security Officers, under management direction and consistent with Consortium Policy, to declaratively control the transactions that are logged.~~
Discussed at Kick Off meeting. See Rules and Requirements Document for logging (99 - 103).
- 2.1.38 The Broker web site shall capture the following information:
 - 2.1.38.1 Date/time of transaction
 - 2.1.38.2 User who performed the transaction
 - 2.1.38.3 Transaction performed

- 2.1.38.4 Location or station as available (e.g. IP Address)
- 2.1.39 The Broker web site shall log the following data for all authentication events:
 - 2.1.39.1 User attempting to authenticate
 - 2.1.39.2 Date/time of transaction
 - 2.1.39.3 Outcome (success, fail, suspend, etc)
 - 2.1.39.4 Location or station as available (e.g. IP Address)
- 2.1.40 The Broker web site shall generate reports for a user-specified period of time

2.2 Performance and Availability

- ~~2.2.1 That system shall allow for 7 x 24 operation with fixed monthly or weekly maintenance windows permitted. The system shall be available not less than 99.5% in any 30 day period.~~

This is a system requirement not relevant to the Broker as discussed at the kick off.
- 2.2.2 The Broker shall meet at least a 99.9% availability excluding planned outages.
- ~~2.2.3 The system shall send the state and employer/TPA endpoints a maximum of 10 files concurrently~~

No longer applicable due to architecture change
- 2.2.4 The system shall allow for electronic error notifications of SIDES Server activity to appropriate administration/support team.
- 2.2.5 The system shall allow 10 concurrent connections for data transfer between the broker web services and its end points (not 10 concurrent connections per connector for clarification).
- 2.2.6 The Broker web service shall accept one (1) file at a time from the State and Employer/TPA systems. [Affects Endpoint(s) Requirements]
- 2.2.7 The Broker web service shall feed the state and employer/TPA systems endpoint one (1) file at a time. [Affects Endpoint(s) Requirements]
- 2.2.8 The maximum request file size, including attachments, non-encoded, non-encrypted is 8 MB. This is subject to change based on testing [Affects Endpoint(s) Requirements]
- 2.2.9 The maximum response file size, including attachments, non-encoded, non-encrypted is 8 MB. This is subject to change based on testing. [Affects Endpoint(s) Requirements]
- 2.2.10 The handshake messaging between Connectors (State and Employer/TPA) and the Broker is http request/response based. [Affects Endpoint(s) Requirements]
- 2.2.11 The web application response time for local and remote access to the Broker users is 2 seconds (not including Reports or Searches). The remote access response time will be measured within the broker environment on the test system.
- 2.2.12 For Broker hosting, the Vendor shall be either ISO 20000 or ISO 9001 certified

- 2.2.13 The maintenance window is scheduled for 4 consecutive hours on a weekly basis at a time to be agreed by the consortium.

2.3 Design Guidelines

- ~~2.3.1 The Development Vendor must address and document their Best Practices approach to building this application, including use of Design and Behavioral Patterns (e.g., MVC, façade, factory)
Covered in the design guidelines document~~
- ~~2.3.2 The Vendor may make use of 3rd party design, development, and modeling tools, but must avoid use of proprietary extensions unless receiving prior approval from the Consortium
Covered in the design guidelines document~~
- 2.3.3 The Broker design shall log faults/errors and shall not abnormally terminate.
- 2.3.4 The Broker design environment shall handle processor loads and memory management.
- ~~2.3.5 The System design shall support the use of processes and logs that monitor data access, user IDs, locations and transactions performed and whether the result of the transaction was successful or not.
See Rules and Requirements document~~
- ~~2.3.6 The System design shall support log attributes that allow SIDES Consortium to search for known or suspected patterns of abuse and how the logs shall be protected from alteration.
See 7.0 View Reports Use Case~~
- 2.3.7 The system shall maintain session state during web sessions. [Affects Endpoint(s) Requirements]
- ~~2.3.8 The System design should support and use Best Practices in minimizing and insulating the effects of underlying system/ infrastructure changes, including the use of J2EE design patterns
Covered in the design guidelines document~~
- ~~2.3.9 The System design shall support transaction boundaries that promote maintainability and minimize impacts on performance and the relationship of use case realizations to delineate transaction boundaries.
Covered in the design guidelines document~~
- 2.3.10 The System design shall support implementation/deployment packages to maximize coupling and cohesion within, and minimal coupling between implementation/deployment packages
- 2.3.11 The System design shall support implementation/deployment packages into architectural layers to promote loose layer coupling and ease of maintenance
- ~~2.3.12 The Vendor design shall consider the following attachment techniques, and recommend with substantiating rationale to the Consortium the technique for use in the UI SIDES application(s) solution: DIME, SwA, MTOM. The solution must be interoperable with a .NET backend legacy system.
Design Issue - Moved to Technical Architecture Document~~

- 2.3.13 The System design shall address the parsing impact of XML files and messages, the marshalling of objects to XML and un-marshalling XML to objects, and the processing effects of a WS-Security capability that includes XML Digital Signatures and XML Encryption (if used) on performance. [Affects Endpoint(s) Requirements]
- 2.3.14 Each XML file shall adhere to the following naming convention: [Affects Endpoint(s) Requirements]
 - 2.3.14.1 Request: State Abbreviation, Employer/TPA Approved Identifier, date and timestamp of transmission from the state endpoint
Revisit
 - 2.3.14.2 Response: Employer/TPA’s Consortium approved Identifier, State Abbreviation, date and timestamp of transmission from the employer/TPA endpoint
Revisit

2.4 Broker Testing Guidelines

- 2.4.1 Verification that the UI SIDES Applications meet their functional requirements, reliability requirements, and performance requirements
- 2.4.2 Verification that the UI SIDES Applications are implemented to specification during the System Integration Testing
- 2.4.3 Execution of each Broker Test Case or function uses valid and invalid data provided by the States. [Affects Endpoint(s) Requirements]
- 2.4.4 The Broker Test Case will exercise exceptions cleanly and appropriately without abnormal termination.
- 2.4.5 Execution of each Use Case-derived test script(s), exercising all Use Case flows, and using valid and invalid data, and validate the performance of the system as specified in the Use Case-derived test script(s)
- 2.4.6 Validation that the expected results occur when valid data is input into the unit, component and/or system, depending on the stage of development
- 2.4.7 Validation that the appropriate error or warning messages are displayed when invalid data is used throughout the stages of development
- 2.4.8 Validation that each business rule is applied correctly
- 2.4.9 Execution of Unit Tests that verify the reliability of individual code modules, libraries, compiled resources, controls, and any other related software executable
- 2.4.10 Execution of Performance Tests that verify that the UI SIDES Applications will perform under heavy loads according to load test scripts.
- 2.4.11 The Vendor shall execute each performance test case in single user, multi-user and mixed-load multi-user simulations according to load test scripts. Mixed-load is to include both web service and web user actions at the same time.
- 2.4.12 Execution of Security Tests that verify that the UI SIDES Applications will be protected from unauthorized access and willful damage, whether the unauthorized access is from internal or external systems, users accessing UI SIDES Application from the Internet

- 2.4.13 Execution of System Integration Tests that verify that the parts of the integrated UI SIDES Applications function together per specification
- 2.4.14 Execution of Installation Tests that verify that the UI SIDES Applications can work correctly with different types of browsers and operating systems as specified in the Rules and Requirements document.
- 2.4.15 Execute Test Cases utilizing black box, white box, boundary value analysis, and equivalence class partitioning techniques, as appropriate
- 2.4.16 Test cases must exist that use consortium provided data to compare validation (schema and business rules) processing results between the States, Broker and Employer/TPA for both request and response files.
[Affects Endpoint(s) Requirements]
- 2.4.17 The Vendor shall document the results of each test case. For each set of test cases executed, the following results shall be documented and maintained:
 - 2.4.17.1 The Vendor shall document the Test Identification Number, if the test is successful
 - 2.4.17.2 The Vendor shall document the Test Identification Number and any error identification information, if the test failed
 - 2.4.17.3 The Vendor shall document the result of the test - Passed, Failed, Not Executable, and For Retest
 - 2.4.17.4 The Vendor shall document the log of the test
 - 2.4.17.5 The Vendor shall document the date of execution for a test
 - 2.4.17.6 The Vendor shall identify the tester who performed the test
 - 2.4.17.7 The Vendor shall track all defects and provide the SIDES Consortium with defect reporting.
- 2.4.18 Defects in any tests shall be logged, tracked, triaged and eliminated.
- 2.4.19 Regression testing shall be employed to test specific conditions which produced these defects. The Vendor shall:
 - 2.4.19.1 Document all defects found during testing into the Change Request/Defect History repository
 - 2.4.19.2 Document all defects against specific Builds and Products and capture supporting documentation, if appropriate
 - 2.4.19.3 Provide reports to the SIDES Consortium that measure the number of defects by status, category, tester, module and other reporting criteria, necessary to provide the SIDES Consortium insight into the software development and testing processes
 - 2.4.19.4 Report any critical defects or other problems likely to impact testing, iteration, or overall project schedule to the SIDES Consortium
- 2.4.20 During triage of defects, the vendor shall use all mechanisms and resources available to them including, but not limited to:
 - 2.4.20.1 Requirements Documentation
 - 2.4.20.2 Design Documentation
 - 2.4.20.3 Physical environment and user observation
- 2.4.21 The vendor shall create and disseminate to the SIDES Consortium progress reports that summarize testing activity. The progress status

report will be compiled at least bi-weekly and shall contain the following content:

- 2.4.21.1 The progress-to-date of testing activities
- 2.4.21.2 The summary of test executions to date
- 2.4.21.3 The number and type of defects detected (Severity I, Severity II, Severity III)
- 2.4.21.4 Any upcoming testing activities what will be performed during the next period
- 2.4.21.5 The Vendor shall identify any testing issues or risks.
- 2.4.22 The Vendor is responsible for correcting any deficiencies in implementation, design or integration and thoroughly managing all versioning of the specific units, components and release candidates.
- 2.4.23 Regression testing procedures shall be instituted to record and subsequently test any detected failures, defects or inadequacies found during the execution of any test case, whether it be a required test or not.
- 2.4.24 Any planned changes to the production environment due to delivery and installation of iteration work products shall require User Acceptance Testing. [Affects Endpoint(s) Requirements]

2.5 Usability

- 2.5.1 The Broker web site shall allow all on-screen actions to be performed by both the keyboard and the mouse.
- 2.5.2 The Broker web site shall allow the user to scroll through data entry items prior to commitment, rather than a page by page commitment where appropriate.
- 2.5.3 The Broker web site shall show which field has cursor control.
- 2.5.4 The Broker web site shall auto-tab in an organized fashion within supported browser capabilities.
- 2.5.5 The Broker web site shall display the format for input in the label for each text box. The broker website will validate against that format. For example dates shall be entered as ‘MMDDYYYY’. The Broker web site will display text entered in a manner to be agreed in design phase.
- ~~2.5.6 The Broker shall check inputs for contradictory or logical problems before submission.~~
Deleted – subsumed in 2.5.7
- 2.5.7 The Broker web site shall ensure that all answers to the dialogue are validated as required, recorded with date stamp and user id and committed.
- ~~2.5.8 The system shall provide a mechanism to allow the user to enable and disable application alerts, prompts, cues, and maintain the users’ preferences regarding those settings where applicable.~~
As agreed to in the kick off meeting, access dictated by role.
- 2.5.9 The Broker web site shall maintain any previously captured data that may have been entered in a “pending” state during a session.

- 2.5.10 The Broker web site shall provide the capability for the **ACTOR** to verify and validate all entered information and confirm the information is correct before committing.
- 2.5.11 The Broker web site shall provide Hover Text for appropriate Internet and Intranet client screen items.
- 2.5.12 The Broker web site shall provide dropdown lists which shall be used where applicable and shall contain both descriptive text and system codes where applicable in the display fields.
- 2.5.13 ~~The system shall comply with all security requirements.~~
Duplicative
- 2.5.14 The Broker web site shall, when displaying tabular or list information, provide column headings. The user may sort on column headings
- 2.5.15 The Broker web site shall provide, where feasible and reasonable, a mechanism to Print the contents of a window/screen, or an entire listing.
- 2.5.16 The Broker web site shall provide, where feasible and reasonable and within supported browser capabilities, a mechanism to Cut, Copy and Paste application information that is displayed.
- 2.5.17 The Broker web site shall provide standard keystroke shortcuts to enable efficient navigation, data entry, and/or context switching, etc within supported browser capabilities.

2.6 Data Transactions

- 2.6.1 The system shall be transaction-based. The user shall enter, update, or delete data on a form and then submit it to the System.
- 2.6.2 The system shall provide strict transaction control allowing for data to be committed if all systems and/or subsystems respond they are ready to commit or to rollback the transaction if any system and/or subsystem does not or cannot respond to the commit request.

2.7 Online Help

- 2.7.1 The Broker web site should provide a mechanism to turn online help on/off at each user's discretion where applicable.
Talked about this in the Kick Off meeting, help will be available by clicking on the help sections.
- 2.7.2 The Broker web site should provide context-sensitive help for each data entry location on each screen.
Talked about this in the Kick Off meeting, help will be available by clicking on the help sections.
- 2.7.3 ~~Make available standard web help application.~~
Will conform to 2.7.1 and 2.7.2

2.8 Accessibility

- 2.8.1 The Broker web site shall comply with the Section 508 Standard of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) by designing each web screen to be readable by the JAWS screen reader.

2.9 Metrics

~~2.9.1 Connector Table Lookup Failure~~

~~Every time a State requests an Employer/TPA URI which does not appear in the Connector Table, a log record must be created with the following data:~~

- ~~• Date and Timestamp~~
- ~~• Sending State~~
- ~~• Request File GUID~~
- ~~• Request Record GUID~~
- ~~• Request Employer/TPA Unique Id~~

~~2.9.2 File Transfer Metrics~~

~~For every attempted file transmission from Connector to Broker, the Broker must maintain a record of success or failure containing the following data:~~

- ~~• Date and Timestamp~~
- ~~• Sending Connector Routing ID~~
- ~~• Destination Connector Routing ID~~
- ~~• Success/Failure Indicator~~
- ~~• Reason for Failure through Codes (if applicable)~~
- ~~• Number of Records Sent~~
- ~~• File Size~~

~~2.9.3 XML Validation Failures~~

~~Every record in an XML request or response file which fails XML schema validation must be logged with the following data:~~

- ~~• Date and Timestamp~~
- ~~• File GUID~~
- ~~• Record GUID~~
- ~~• Originator~~
- ~~• Destination (and destination Connector Routing ID if applicable)~~
- ~~• Record~~
- ~~• Reason for Failure through Codes~~

2.10 Logging Data

~~2.10.1 Connector Table Journal Data~~

~~Every time an entry in the Connector Table is created, updated, or deleted a log record must be created. The log record must include the following data:~~

- ~~• Date and Timestamp~~
- ~~• Routing ID~~
- ~~• New URI~~
- ~~• Old URI (if applicable)~~
- ~~• Activity Type (Create, Update, or Delete)~~
- ~~• Actor (Admin that performed the action)~~

Deprecated

Each state will share authentication credentials for a single employer.