RETS Certification System
RETS 1.7.2 and 1.8 Testing Rules

Version: 02

June 2014

Table of Contents

1 RETS 1.7.2 and 1.8 Certification System Introduction....3
1.1 Glossary....3
1.2 Certification Flow (Summary)....4
2 RETS 1.7.2 Standards....5
2.1 RETS 1.7.2 Client Compliance Rules....5
2.2 RETS 1.7.2 Client Certification Rules....6
2.3 RETS 1.7.2 Server Compliance Rules....7
2.4 RETS 1.7.2 Server Certification Rules....10
3 RETS 1.8 Standards....12
3.1 RETS 1.8 Client Compliance Rules....12
3.2 RETS 1.8 Client Certification Rules....13
3.3 RETS 1.8 Server Compliance Rules....14
3.4 RETS 1.8 Server Certification Rules....18
4 RETS 1.x Report Cards....19

1 RETS 1.7.2 and 1.8 Certification System Introduction

This document contains the RETS Compliance requirements an applicant's RETS 1.72 and 1.8 implementation would need to satisfy before receiving RESO Certification.

This document should be read by any organization who wants:

- To know the changes required to have compliant RETS 1.7.2 or 1.8 Client or Server.
- To have an understanding of the certification process.

Receiving RETS 1.7.2 and 1.8 Certification is a multiple step process that begins with an application submitted through http://reso.org/certification.

This document focuses on the standards the Compliance Department and Certification Department will follow through the certification process. The content of this document was determined by various RESO Compliance Workgroup(s).

1.1 Glossary

RETS 1.7.2/1.8 Client Compliance Rules: A set of rules applied to an applicant's RETS client to determine if it adheres to and is compliant with the appropriate RETS 1.x standard.

RETS 1.7.2/1.8 Client Certification: An applicant is awarded a RETS certificate if that applicant's metadata adheres to the set of RETS Compliance Rules as dictated by this workgroup.

RETS 1.7.2/1.8 Server Compliance Rules: A set of rules applied to an applicant's RETS Server to determine if it adheres to and is compliant with the appropriate RETS 1.x standard.

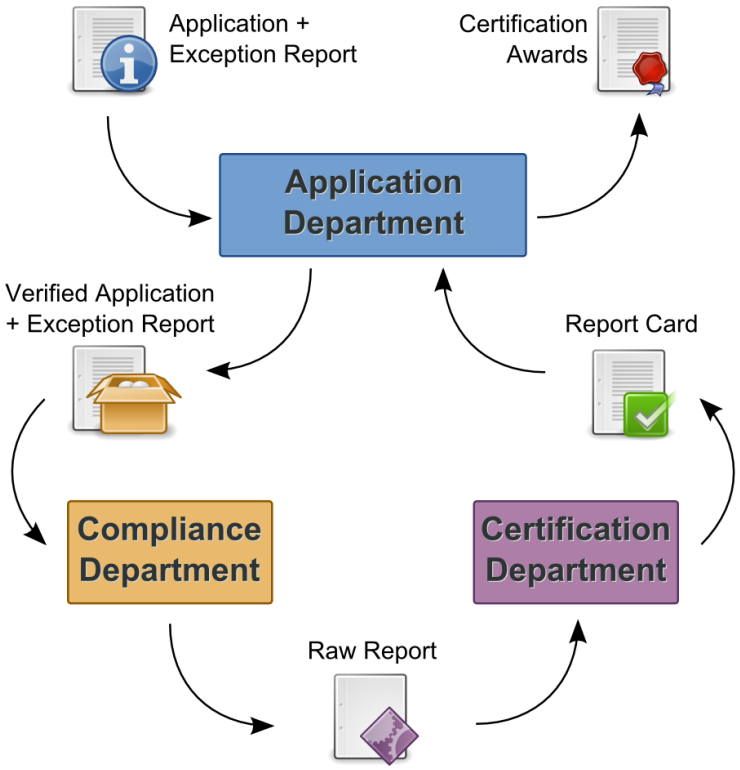
RETS 1.7.2/1.8 Server Certification: An applicant is awarded a RETS certificate if that applicant's metadata adheres to the set of RETS Compliance Rules as dictated by this workgroup.

Compliance Requirement IDs: Each rule is identified by a unique ID. They take the format similar to "**COMP-R###X-XXX-#**" and are found immediately before the rule.

Certification Requirement IDs: Each rule is identified by a unique ID. They take the format similar to "**REQ-R###X-XXX-#**" and are found immediately before the rule.

The IDs are provided to help those discussing these rules to identify rules in this document. "###X" is replaced by the RETS Standard and platform: R172C & R172S (for RETS 1.7.2 Clients and Servers), R180C & R180S (for RETS 1.8.0 Clients and Servers),

1.2 Certification Flow (Summary)



Certification Flow	Group	Action	Output
1: Application Processing (Pre-Certification)	**Application Department**	Accept and Verify Applicant's ***'Certification Application''*** via reso.org/certification	Prepare for Compliance Testing. Pass application to Compliance Department. *(Exception Report not required for Client Certification.)*
2: Compliance Testing	**Compliance Department**	Test applicant's metadata against well-defined Compliance Rules as set forth by the DD Compliance Workgroup.	Testing results formatted in ***'Raw Report'*** package. Pass ***'Raw Report'*** to Certification Department.
3: Certification Analysis	**Certification Department**	Analyze ***'Raw Report'*** to determine if applicant qualifies for a certificate. Create a ***'Report Card'*** with findings.	Pass analysis results and ***'Report Card'*** back to Application Processing.
4: Application Processing (Post-Certification)	**Application Department**	Act on Certification Department recommendation	Notify applicant of Certificate Pass/Fail. Send notification and ***'Report Card'*** back to Applicant.

2 RETS 1.7.2 Standards

2.1 RETS 1.7.2 Client Compliance Rules

This section contains all of the rules that RESO will use in the Compliance testing. The specific set of rules that need must be passed for a "Certification" are discussed in the next section.

2.1.1 General Compliance Information

These tests are applicable to all RETS Transactions. They validate the Request Format, the required request header fields, and optional client request header fields.

COMP-R172C -G-1: The client MUST provide all HTTP request in the format specified in Section 3.2 of the RETS 1.7.2 specification.

COMP-R172C-G-2: The client HTTP Requests MUST contain the required Request Header fields as specified in Section 3.2 of the RETS 1.7.2 specification.

COMP-R172C-G-3: The client HTTP Requests MAY contain optional Request Header fields are used as specified in Section 3.3 of the RETS 1.7.2 specification. If provided, the optional header fields MUST be formatted as specified.

2.1.2 Compliance Info: Login

COMP-R172C-LI-1: The client MUST provide a correctly formatted Login transaction as described in Section 4 of the RETS 1.7.2 specification.

COMP-R172C-LI-2: The client MAY provide the optional request arguments as specified in section 4.4 of the RETS 1.7.2 specification. If provided, the optional request arguments MUST be formatted as specified.

COMP-R172C-LI-3: The client MUST issue a login request before proceeding with any other. (The login transaction verifies user information and begins a RETS session.)

2.1.3 Compliance Info: GetObject

COMP-R172C-GO-1: The client MUST provide the required header fields as defined in Section 5.1 of the RETS 1.7.2 specification. (No optional header fields are specified.)

COMP-R172C-GO-2: The client MUST provide the required arguments as defined in Section 5.3 of the RETS 1.7.2 specification.

COMP-R172C-GO-4: The client MAY provide the optional request arguments as defined in Section 5.4 of the RETS 1.7.2 specification. If provided, the optional request arguments MUST be formatted as specified.

2.1.4 Compliance Info: Logout

COMP-R172C-LO-1: The client MUST provide a correctly formatted Logout transaction as described in Section 6 of the RETS 1.7.2 specification. (There are no required or optional request arguments to specify.)

2.1.5 Compliance Info: Search

COMP-R172C-S-1: The client MUST provide the required request arguments as defined in Section 7.3 of the RETS 1.7.2 specification.

COMP-R172C-S-2: The client MAY provide the optional request arguments as stated in Section 7.4 of the RETS 1.7.2 specification. If provided, the optional request arguments MUST be formatted as specified.

COMP-R172C-S-3: The client MUST provide the search queries with the language and in the format as specified in Section 7.6 of the RETS 1.7.2 specification.

2.1.6 Compliance Info: GetMetadata

COMP-R172C-GM-1: The client will provide the required arguments as defined in Section 12.2 of the RETS 1.7.2 specification.

COMP-R172C-GM-2: The client MAY provide the optional request arguments as defined in Section 12.3 of the RETS 1.7.2 specification. If provided, the optional request arguments MUST be formatted as specified.

2.2 RETS 1.7.2 Client Certification Rules

This section contains all of the rules that RESO will use in the Compliance testing. The specific set of rules that need must be passed for a "Certification" are discussed in the next section.

These tests confirms that certification candidates implement the required headers and fields of the RETS 1.7.2 standard and the required minimum actions described in the RETS specification for the sections listed below. Optional headers, fields and actions are not covered by the compliance test.

2.2.1 General Certification Test(s)

REQ-R172C-G-1: All MUST requirements specified in the Compliance section above MUST be satisfied unless specified differently in other Certification requirements below.

2.2.2 Certification Details: Login Test(s)

REQ-R172C-LI-1: The RETS Reply Code “0” from the RETS server for a Login transaction is necessary for compliance.

2.2.3 Certification Details: GetObject Test(s)

REQ-R172C-GO-1: The RETS Reply Code “0” from the RETS server for a GetObject transaction is necessary for compliance.

2.2.4 Certification Details: Logout Test(s)

REQ-R172C-LO-1: The RETS Reply Code “0” from the RETS server for a Logout transaction is necessary for compliance.

2.2.5 Certification Details: Search Test(s)

REQ-R172C-S-1: The RETS Reply Code “0” from the RETS server for a Search transaction is necessary for compliance.

> **Note:** The RETS Reply Code “20206” from the RETS server signifies an invalid query syntax. This will cause the RETS Client to fail this test. See section 7.7 of the RETS 1.7.2 specification for details.

2.2.6 Certification Details: GetMetadata Test(s)

REQ-R172C-GM-1: The RETS Reply Code “0” from the RETS server for a GetMetadata transaction is necessary for compliance.

2.2.7 Certification Details: GetPayloadList Test(s)

REQ-R172C-GPL-1: The RETS Reply Code “0” from the RETS server for a GetPayload transaction is necessary for compliance.

2.2.8 Non-Certified Functionality

The following RETS 1.7.2 Client functionality will be ignored for Certification: ChangePassword (Section 9); Update (Section 10)

2.3 RETS 1.7.2 Server Compliance Rules

This section contains all of the rules that RESO will use in the Compliance testing. The specific set of rules that need must be passed for a "Certification" are discussed in Section 3.

2.3.1 General Compliance Information

These tests are applicable to all RETS Transactions. They validate the Response Format, the required response header fields, and optional client response header fields.

COMP-R172S-G-1: The server MUST provide all HTTP responses in the format specified in Section 3.5 of the RETS 1.7.2 specification.

COMP-R172S-G-2: The server HTTP Responses MUST contain the required Response Header fields as specified in Section 3.6 of the RETS 1.7.2 specification.

COMP-R172S-G-3: The client HTTP Responses MAY contain optional Response Header fields are used as specified in Section 3.7 of the RETS 1.7.2 specification. If provided, the optional header fields MUST be formatted as specified.

2.3.2 Compliance Info: Login

COMP-R172S-LI-1: The RETS Server MUST use the required response header fields as defined in Section 4.5 of the RETS 1.7.2 specification.

COMP-R172S-LI-2: The RETS Server MUST use the required response arguments as defined in Section 4.7 of the RETS 1.7.2 specification.

COMP-R172S-LI-3: The RETS Server MAY use optional response arguments. If the optional response arguments are provided in the server’s response, they MUST functions as defined in Section 4.8 of the RETS 1.7.2 specification.

COMP-R172S-LI-4: The RETS Server MUST use the valid login response format as defined in Section 4.6 of the RETS 1.7.2 specification. The Session Information Tokens (RCP 65) MUST be used to be considered compliant. Older deprecated methods MAY be used for backward compatibility purposes.

COMP-R172S-LI-5: The RETS Server MUST allow for different forms of authentication, including: Basic Authentication, Digest Authentication, and UA-Authentication.

COMP-R172S-LI-6: The RETS Server MUST report the required capability URLS: Login, Search, and GetMetadata.

COMP-R172S-LI-7: The RETS Server MAY report the optional capability URLS: Action, ChangePassword, GetObject, LoginComplete, and Update.

COMP-R172S-LI-8: The RETS Server MUST provide date formats in the response header close to NOW in GMT time. **NOTE:** Time variation allowance specified in Certification Requirements.

2.3.3 Compliance Info: GetObject

COMP-R172S-GO-1: The RETS Server MUST use the required response header fields as defined in Section 5.5 of the RETS 1.7.2 specification.

COMP-R172S-GO-2: The RETS Server MAY use optional response header fields. If the optional response header fields are provided in the server's response, they MUST function as defined in Section 5.6 of the RETS 1.7.2 specification.

COMP-R172S-GO-3: The RETS Server MUST use Multipart Responses as defined in Section 5.11 of the RETS 1.7.2 specification including their format, general construction, and error handling capabilities. Also, the content-type MUST be multipart and parallel.

2.3.4 Compliance Info: Logout

COMP-R172S-LO-1: The RETS Server use the required response arguments as defined in Section 6.3 of the RETS 1.7.2 specification.

COMP-R172S-LO-2: The RETS Server MAY use optional response arguments. If the optional response arguments are provided in the server's response, they MUST function as defined in Section 6.4 of the RETS 1.7.2 specification.

COMP-R172S-LO-3: The RETS Server MUST use the logout response format as defined as defined in Section 6.5 of the RETS 1.7.2 specification.

COMP-R172S-LO-4: If the client sends a Logout transaction, the server MUST attempt to send a response before terminating the session with the RETS Server Testing Tool.

COMP-R172S-LO-5: The server MAY send accounting information back to the client in the response to a logout request transaction. **NOTE:** The client is not required to display or otherwise process the accounting information.

2.3.5 Compliance Info: Search

COMP-R172S-S-1: The RETS Server MUST use the required response header fields as defined in Section 3.6 of the RETS 1.7.2 specification including "date", "cache-control", "content-type", and "rets-version".

COMP-R172S-S-2: The RETS Server MAY use optional response header fields. If the optional header fields are provided in the server's response, they MUST function as defined in Section 3.7 of the RETS 1.7.2 specification if provided in the server's response including "content-length", "transfer-encoding", and "server".

COMP-R172S-S-3: The RETS Server MUST use the search response format as defined in Section 7.6 of the RETS 1.7.2 specification.

COMP-R172S-S-4: The RETS Server MUST use the search result "count" functionality as specified in section 7.4.1 of the RETS 1.7.2 specification.

COMP-R172S-S-5: The RETS Server MUST return search results data in one of three formats: COMPACT, COMPACT-DECODED or STANDARD-XML. The XML responses MAY be validated against the appropriate DTD, based on format. (Section 7.4.2).

COMP-R172S-S-6: The RETS Server MUST provide search result "limit" functionality as specified in Section 7.4.3 of the RETS 1.7.2 specification.

COMP-R172S-S-7: The RETS Server MAY provide search result “offset” functionality as specified in Section 7.4.4 of the RETS 1.7.2 specification.

> **Note:** Offset is an optional request argument and support for this is NOT required in 1.8. The server's metadata contains a flag indicating if offset is available for the server. This requirement has been changed from MUST to MAY.

COMP-R172S-S-8: The RETS Server MUST provide search result “select” functionality as specified in Section 7.4.5 of the RETS 1.7.2 specification.

COMP-R172S-S-9: The RETS Server MUST provide search result “RestrictedIndicator” functionality as specified in Section 7.4.6 of the RETS 1.7.2 specification.

COMP-R172S-S-10: The RETS Server MUST accept RETS queries with system names and standard names as specified in Section 7.4.7 of the RETS 1.7.2 specification.

COMP-R172S-S-11: The RETS Server MUST properly use the Query and QueryType functionality as specified in Sections 7.3.2 of the RETS 1.7.2 specification.

COMP-R172S-S-12: The RETS Server MUST have DMQL2 support by allowing queries using (1) StandardName, (2) SystemNames (Compact Decoded), and (3) both.

COMP-R172S-S-13: The RETS Server MUST have DMQL2 Query parameter support for numeric testing with following query types: “Greater than”, “Less than”, and “Range”.

COMP-R172S-S-14: The RETS Server MUST have DMQL2 Query parameter support for character testing with following query types: “AND”, “OR”, “Contains”, and “Starts With”.

COMP-R172S-S-15: The RETS Server MUST have DMQL2 Query parameter support for date testing with following query types: “After this date”, “Before this date”, and “Today”.

COMP-R172S-S-16: The RETS Server MUST have DMQL2 Query parameter support for time zone offsets. (Section 7.7.2).

COMP-R172S-S-17: The RETS Server MUST have DMQL2 Query parameter support for the “.EMPTY.” and “.ANY.” session information tokens (Section 7.7.2).

COMP-R172S-S-18 (Catch-All): The RETS Server MUST support any MUST requirement found within the RETS 1.7.2 specification not found within this document.

2.3.6 Compliance Info: Update

COMP-R172S-U-1: The RETS Server MUST use the update response format as defined as defined in Section 10.5 of the RETS 1.7.2 specification (well-formed XML).

COMP-R172S-U-2: The RETS Server MUST use the correct formats (well-formed XML) for Error and Warning blocks that are returned to the client.

COMP-R172S-U-3: The RETS Server MUST use the format and the presence of the required elements of the Update Response. The server MAY use a DTD created from the format defined by the specification.

COMP-R172S-U-4: A RETS Server’s Update functionality MAY have validation within the metadata. If it does, this Validation section MUST be formatted properly.

2.3.7 Compliance Info: Metadata

COMP-R172S-MD-1: The RETS Server MUST use required response header fields as defined in Section 12.4 of the RETS 1.7.2 specification ("date", "cache-control", "content-type", "rets-version").

COMP-R172S-MD-2: The RETS Server MUST use required response arguments as defined in Section 12.5 of the RETS 1.7.2 specification ("content-length", "transfer-encoding", "server").

COMP-R172S-MD-3: The RETS Server MAY use optional response arguments. If the optional response arguments are provided in the server's response, they MUST function as defined in Section 12.6 of the RETS 1.7.2 specification.

COMP-R172S-MD-4: The RETS Server MUST use the Metadata standard XML response format as defined in Sections 11 and 12.7 of the RETS 1.7.2 specification and validated against the published RESO DTD for standard XML.

COMP-R172S-MD-5: The RETS Server MUST use the Metadata's Compact Data response format as defined in Sections 13.1, 13.2, and 13.3 of the RETS 1.7.2 specification and validated against the published RESO DTD for compact data XML.

COMP-R172S-MD-6: The RETS Server MUST allow the following types of arguments with support for IDs of 0 and *: METADATA-SYSTEM, METADATA-RESOURCE, and METADATA-CLASS.

COMP-R172S-MD-7: The RETS Server MUST use the response formats and respond to queries for the ID: METADATA-SYSTEM, METADATA-RESOURCE, and METADATA-CLASS.

COMP-R172S -MD-8: The RETS Server MUST support user configured Id parameter for METADATA-CLASS:METADATA-TABLE.

2.4 RETS 1.7.2 Server Certification Rules

This section contains all of the rules that RESO will use in the Compliance testing. The specific set of rules that need must be passed for a "Certification" are discussed in the next section.

These tests confirms that certification candidates implement the required headers and fields of the RETS 1.7.2 standard and the required minimum actions described in the RETS specification for the sections listed below. Optional headers, fields and actions are not covered by the compliance test.

2.4.1 General Certification Requirements

REQ-R172S-GCR-1: The RETS Server MUST provide the correct reply codes when invalid requests are made (generic negative testing). This requirement applies to each of the certification test sections found in this document.

> **NOTE:** Details on the reply codes are found in many locations throughout the RETS 1.7.2 Specification. Details on Negative Tests performed by the RESO Server Testing Tool can be found in the functional requirements document. Additional details may be provided below, as required for clarification.

2.4.2 Certification Details: Login Test(s)

REQ-R172S-LI-1: The RETS Reply Code "0" from the RETS server is necessary for compliance.

REQ-R172S-LI-2: The RETS Server MUST be within 30 minutes of GMT (before or after). The datetime information in the Login response will be used to determine the server's time.

2.4.3 Certification Details: GetObject Test(s)

REQ-R172S-GO-1: The RETS Reply Code "0" from the RETS server is necessary for compliance.

2.4.4 Certification Details: Logout Test(s)

REQ-R172S-LO-1: The RETS Reply Code “0” from the RETS server is necessary for compliance.

2.4.5 Certification Details: Search Test(s)

REQ-R172S-S-1: The RETS Reply Code “0” from the RETS server is necessary for compliance.

> **Note:** The RETS Reply Code “20206” from the RETS server signifies an invalid query syntax. This will case the RETS Client to fail this test. See section 7.7 of the RETS 1.7.2 specification for details.

2.4.6 Certification Details: Update Test(s)

NOTE: Update Functionality is not included in current server certifications.

2.4.7 Certification Details: Metadata Test(s)

REQ-R172S-GM-1: The RETS Reply Code “0” from the RETS server is necessary for compliance.

2.4.8 Non-Certified Functionality

The following RETS 1.7.2 Server functionality will be ignored for Certification: ChangePassword (Section 9); Update (Section 10)

> **DEFERRED:** DMQL2 Time Zone Offsets (7.7.2); DMQL2 “.EMPTY.” session information token

3 RETS 1.8 Standards

3.1 RETS 1.8 Client Compliance Rules

This section contains all of the rules that RESO will use in the Compliance testing. The specific set of rules that need must be passed for a "Certification" are discussed in the next section.

3.1.1 General Compliance Information

These tests are applicable to all RETS Transactions. They validate the Request Format, the required request header fields, and optional client request header fields.

COMP-R180C-G-1: The client MUST provide all HTTP request in the format specified in Section 3.2 of the RETS 1.8 specification.

COMP-R180C-G-2: The client HTTP Requests MUST contain the required Request Header fields as specified in Section 3.3 of the RETS 1.8 specification.

COMP-R180C-G-3: The client HTTP Requests MAY contain optional Request Header fields are used as specified in Section 3.4 of the RETS 1.8 specification. If provided, the optional header fields MUST be formatted as specified.

3.1.2 Compliance Info: Login

COMP-R180C-LI-1: The client MUST provide a correctly formatted Login transaction as described in Section 4 of the RETS 1.8 specification.

COMP-R180C-LI-2: The client MAY provide the optional request arguments as specified in section 4.4 of the RETS 1.8 specification. If provided, the optional request arguments MUST be formatted as specified.

COMP-R180C-LI-3: The client MUST issue a login request before proceeding with any other. (The login transaction verifies user information and begins a RETS session.)

3.1.3 Compliance Info: GetObject

COMP-R180C-GO-1: The client MUST provide the required header fields as defined in Section 5.1 of the RETS 1.8 specification. (No optional header fields are specified.)

COMP-R180C-GO-2: The client MUST provide the required arguments as defined in Section 5.3 of the RETS 1.8 specification.

COMP-R180C-GO-4: The client MAY provide the optional request arguments as defined in Section 5.4 of the RETS 1.8 specification. If provided, the optional request arguments MUST be formatted as specified.

3.1.4 Compliance Info: Logout

COMP-R180C-LO-1: The client MUST provide a correctly formatted Logout transaction as described in Section 6 of the RETS 1.8 specification. (There are no required or optional request arguments to specify.)

3.1.5 Compliance Info: Search

COMP-R180C-S-1: The client MUST provide the required request arguments as defined in Section 7.3 of the RETS 1.8 specification.

COMP-R180C-S-2: The client MAY provide the optional request arguments as stated in Section 7.4 of the RETS 1.8 specification. If provided, the optional request arguments MUST be formatted as specified.

COMP-R180C-S-3: The client MUST provide the search queries with the language and in the format as specified in Section 7.6 of the RETS 1.8 specification.

3.1.6 Compliance Info: GetMetadata

COMP-R180C-GM-1: The client will provide the required arguments as defined in Section 12.2 of the RETS 1.8 specification.

COMP-R180C-GM-2: The client MAY provide the optional request arguments as defined in Section 12.3 of the RETS 1.8 specification. If provided, the optional request arguments MUST be formatted as specified.

3.1.7 Compliance Info: GetPayloadList

COMP-R180C-GPL-1: The client MUST provide a correctly formatted GetPayloadList transaction as described in Section 14 of the RETS 1.8 specification.

COMP-R180C-GPL-2: The client MAY provide the optional request arguments as defined in Section 14.2 of the RETS 1.8 specification. If provided, the optional request arguments MUST be formatted as specified.

3.2 RETS 1.8 Client Certification Rules

This section contains all of the rules that RESO will use in the Compliance testing. The specific set of rules that need must be passed for a "Certification" are discussed in the next section.

These tests confirms that certification candidates implement the required headers and fields of the RETS 1.8 standard and the required minimum actions described in the RETS specification for the sections listed below. Optional headers, fields and actions are not covered by the compliance test.

3.2.1 General Certification Test(s)

REQ-R180C-G-1: All MUST requirements specified in the Compliance section above MUST be satisfied unless specified differently in other Certification requirements below.

3.2.2 Certification Details: Login Test(s)

REQ-R180C-LI-1: The RETS Reply Code “0” from the RETS server for a Login transaction is necessary for compliance.

3.2.3 Certification Details: GetObject Test(s)

REQ-R180C-GO-1: The RETS Reply Code “0” from the RETS server for a GetObject transaction is necessary for compliance.

3.2.4 Certification Details: Logout Test(s)

REQ-R180C-LO-1: The RETS Reply Code “0” from the RETS server for a Logout transaction is necessary for compliance.

3.2.5 Certification Details: Search Test(s)

REQ-R180C-S-1: The RETS Reply Code “0” from the RETS server for a Search transaction is necessary for compliance.

> **Note:** The RETS Reply Code “20206” from the RETS server signifies an invalid query syntax. This will cause the RETS Client to fail this test. See section 7.6 of the RETS 1.8 specification for details.

3.2.6 Certification Details: GetMetadata Test(s)

REQ-R180C-GM-1: The RETS Reply Code “0” from the RETS server for a GetMetadata transaction is necessary for compliance.

3.2.7 Certification Details: GetPayloadList Test(s)

REQ-R180C-GPL-1: The RETS Reply Code “0” from the RETS server for a GetPayload transaction is necessary for compliance.

3.2.8 Non-Certified Functionality

The following RETS 1.8 Client functionality will be ignored for Certification: ChangePassword (Section 9); Update (Section 10); PostObject (Section 13); GetPayloadList (Section 14)

3.3 RETS 1.8 Server Compliance Rules

This section contains all of the rules that RESO will use in the Compliance testing. The specific set of rules that need must be passed for a "Certification" are discussed in the following section.

3.3.1 General Compliance Information

These tests are applicable to all RETS Transactions. They validate the Response Format, the required response header fields, and optional client response header fields.

COMP-R180S-GT-1: The server MUST provide all HTTP responses in the format specified in Section 3.5 of the RETS 1.8 specification.

COMP-R180S-GT-2: The server HTTP Responses MUST contain the required Response Header fields as specified in Section 3.6 of the RETS 1.8 specification.

COMP-R180S-GT-3: The client HTTP Responses MAY contain optional Response Header fields are used as specified in Section 3.7 of the RETS 1.8 specification. If provided, the optional header fields MUST be formatted as specified.

3.3.2 Compliance Info: Login

COMP-R180S-LI-1: The RETS Server MUST use the required response header fields as defined in Section 4.5 of the RETS 1.8 specification.

COMP-R180S-LI-2: The RETS Server MUST use the required response arguments as defined in Section 4.7 of the RETS 1.8 specification.

COMP-R180S-LI-3: The RETS Server MAY use optional response arguments. If the optional response arguments are provided in the server’s response, they MUST functions as defined in Section 4.8 of the RETS 1.8 specification.

COMP-R180S-LI-4: The RETS Server MUST use the valid login response format as defined in Section 4.6 of the RETS 1.8 specification. The Session Information Tokens (RCP 65) MUST be used to be considered compliant. Older deprecated methods MAY be used for backward compatibility purposes.

COMP-R180S-LI-5: The RETS Server MUST allow for different forms of authentication, including: Basic Authentication, Digest Authentication, and UA-Authentication.

COMP-R180S-LI-6: The RETS Server MUST report the required capability URLS: Login, Search, and GetMetadata.

COMP-R180S-LI-7: The RETS Server MAY report the optional capability URLS: Action, ChangePassword, GetObject, LoginComplete, Update, PostObject, and GetPayloadList.

COMP-R180S-LI-8: The RETS Server MUST provide date formats in the response header close to NOW in GMT time. **NOTE:** Time variation allowance specified in Certification Requirements.

3.3.3 Compliance Info: GetObject

COMP-R180S-GO-1: The RETS Server MUST use the required response header fields as defined in Section 5.5 of the RETS 1.8 specification.

COMP-R180S-GO-2: The RETS Server MAY use optional response header fields. If the optional response header fields are provided in the server's response, they MUST function as defined in Section 5.6 of the RETS 1.8 specification.

COMP-R180S-GO-3: The RETS Server MUST use Multipart Responses as defined in Section 5.11 of the RETS 1.8 specification including their format, general construction, and error handling capabilities. Also, the content-type MUST be multipart and parallel.

COMP-R180S-GO-4: The RETS Server MUST use ObjectData Classes as defined in Section 5.12 of the RETS 1.8 specification including missing or null arguments and different “Location” values.

3.3.4 Compliance Info: Logout

COMP-R180S-LO-1: The RETS Server use the required response arguments as defined in Section 6.3 of the RETS 1.8 specification.

COMP-R180S-LO-2: The RETS Server MAY use optional response arguments. If the optional response arguments are provided in the server’s response, they MUST function as defined in Section 6.4 of the RETS 1.8 specification.

COMP-R180S-LO-3: The RETS Server MUST use the logout response format as defined as defined in Section 6.5 of the RETS 1.8 specification.

COMP-R180S-LO-4: If the client sends a Logout transaction, the server MUST attempt to send a response before terminating the session with the RETS Server Testing Tool.

COMP-R180S-LO-5: The server MAY send accounting information back to the client in the response to a logout request transaction. **NOTE:** The client is not required to display or otherwise process the accounting information.

3.3.5 Compliance Info: Search

COMP-R180S-S-1: The RETS Server MUST use the required response header fields as defined in Section 7.5 of the RETS 1.8 specification including "date", "cache-control", "content-type", and "rets-version".

COMP-R180S-S-2: The RETS Server MAY use optional response header fields. If the optional header fields are provided in the server’s response, they MUST function as defined in Section 7.5 of the RETS 1.8 specification if provided in the server’s response including "content-length", "transfer-encoding", and "server".

COMP-R180S-S-3: The RETS Server MUST use the search response format as defined in Section 7.5 of the RETS 1.8 specification.

COMP-R180S-S-4: The RETS Server MUST use the search result “count” functionality as specified in section 7.4.1 of the RETS 1.8 specification.

COMP-R180S-S-5: The RETS Server MUST return search results data in one of three formats: COMPACT, COMPACT-DECODED or STANDARD-XML. The XML responses MAY be validated against the appropriate DTD, based on format. (Section 7.4.2).

> **Note:** The Standard Name DTD (REdata.dtd) used to validate the STANDARD-XML formatted responses is not available. Until the DTD becomes available for certification, the STANDARD-XML standard name response data format for the Search transaction will NOT be validated. All system names formats and the COMPACT and COMPACT-DECODED standard name formats will continue to be validated with the available compact DTDs for the Search transaction. *(Note updated April 10, 2014)*

COMP-R180S-S-6: The RETS Server MUST provide search result "limit" functionality as specified in Section 7.4.3 of the RETS 1.8 specification.

COMP-R180S-S-7: The RETS Server MAY provide search result "offset" functionality as specified in Section 7.4.4 of the RETS 1.8 specification.

> **Note:** Offset is an optional request argument and support for this is NOT required in 1.8. The server's metadata contains a flag indicating if offset is available for the server. This requirement has been changed from MUST to MAY. *(Note updated April 10, 2014)*

COMP-R180S-S-8: The RETS Server MUST provide search result "select" functionality as specified in Section 7.4.5 of the RETS 1.8 specification.

COMP-R180S-S-9: The RETS Server MUST provide search result "RestrictedIndicator" functionality as specified in Section 7.4.6 of the RETS 1.8 specification.

COMP-R180S-S-10: The RETS Server MUST accept RETS queries with system names, standard names or mixed system and standard names as specified in Section 7.4.7 of the RETS 1.8 specification.

COMP-R180S-S-11: The RETS Server MUST properly use the Query and QueryType functionality as specified in Sections 7.4.9 and 7.4.10 of the RETS 1.8 specification.

COMP-R180S-S-12: The RETS Server MUST have DMQL2 support by allowing queries using (1) StandardName, (2) SystemNames (Compact Decoded), and (3) both.

COMP-R180S-S-13: The RETS Server MUST have DMQL2 Query parameter support for numeric testing with following query types: "Greater than", "Less than", and "Range".

COMP-R180S-S-14: The RETS Server MUST have DMQL2 Query parameter support for character testing with following query types: "AND", "OR", "Contains", and "Starts With".

COMP-R180S-S-15: The RETS Server MUST have DMQL2 Query parameter support for date testing with following query types: "After this date", "Before this date", and "Today".

COMP-R180S-S-16: The RETS Server MUST have DMQL2 Query parameter support for time zone offsets. (Section 7.6.2).

COMP-R180S-S-17: The RETS Server MUST have DMQL2 Query parameter support for the ".EMPTY." and ".ANY." session information tokens (Section 4.7.5 and RCP 65).

COMP-R180S-S-18 (Catch-All): The RETS Server MUST support any MUST requirement found within the RETS 1.8 specification not found within this document.

3.3.6 Compliance Info: Update

COMP-R180S-U-1: The RETS Server MUST use the update response format as defined as defined in Section 10.5 of the RETS 1.8 specification (well-formed XML).

COMP-R180S-U-2: The RETS Server MUST use the correct formats (well-formed XML) for Error and Warning blocks that are returned to the client.

COMP-R180S-U-3: The RETS Server MUST use the format and the presence of the required elements of the Update Response. The server MAY use a DTD created from the format defined by the specification.

COMP-R180S-U-4: A RETS Server's Update functionality MAY have validation within the metadata. If it does, this Validation section MUST be formatted properly.

3.3.7 Compliance Info: Metadata

COMP-R180S-MD-1: The RETS Server MUST use required response header fields as defined in Section 12.4 of the RETS 1.8 specification ("date", "cache-control", "content-type", "rets-version").

COMP-R180S-MD-2: The RETS Server MUST use required response arguments as defined in Section 12.5 of the RETS 1.8 specification ("content-length", "transfer-encoding", "server").

COMP-R180S-MD-3: The RETS Server MAY use optional response arguments. If the optional response arguments are provided in the server's response, they MUST function as defined in Section 12.6 of the RETS 1.8 specification.

COMP-R180S-MD-4: The RETS Server MUST use the Metadata standard XML response format as defined in Sections 11 and 12.7 of the RETS 1.8 specification and validated against the published RESO DTD for standard XML.

COMP-R180S-MD-5: The RETS Server MUST use the Metadata's Compact Data response format as defined in Sections 15.1, 15.2, and 15.3 of the RETS 1.8 specification and validated against the published RESO DTD for compact data XML.

COMP-R180S-MD-6: The RETS Server MUST allow the following types of arguments with support for IDs of 0 and *: METADATA-SYSTEM, METADATA-RESOURCE, and METADATA-CLASS.

COMP-R180S-MD-7: The RETS Server MUST use the response formats and respond to queries for the ID: METADATA-SYSTEM, METADATA-RESOURCE, and METADATA-CLASS.

COMP-R180S-MD-8: The RETS Server MUST support user configured Id parameter for METADATA-CLASS:METADATA-TABLE.

3.3.8 Compliance Info: PostObject

COMP-R180S-PO-1: The RETS Server MUST use the PostObject response format as defined as defined in Section 13.4 of the RETS 1.8 specification (ResponseBody format).

3.3.9 Compliance Info: GetPayloadList

COMP-R180S-GPL-1: The RETS Server MUST use the GetPayloadList response format as defined as defined in Section 14.5 of the RETS 1.8 specification.

3.4 RETS 1.8 Server Certification Rules

This section contains all of the rules that RESO will use in the Compliance testing. The specific set of rules that need must be passed for a "Certification" are discussed in the next section.

These tests confirms that certification candidates implement the required headers and fields of the RETS 1.8 standard and the required minimum actions described in the RETS specification for the sections listed below. Optional headers, fields and actions are not covered by the compliance test.

3.4.1 General Certification Requirements

REQ-R180S-GCR-1: The RETS Server MUST provide the correct reply codes when invalid requests are made (generic negative testing). This requirement applies to each of the certification test sections found in this document.

> **NOTE:** Details on the reply codes are found in many locations throughout the RETS 1.8 Specification. Details on Negative Tests performed by the RESO Server Testing Tool can be found in the functional requirements document. Additional details may be provided below, as required for clarification.

3.4.2 Certification Details: Login Test(s)

REQ-R180S-LI-1: The RETS Reply Code “0” from the RETS server is necessary for compliance.

REQ-R180S-LI-2: The RETS Server MUST be within 30 minutes of GMT (before or after). The datetime information in the Login response will be used to determine the server’s time.

3.4.3 Certification Details: GetObject Test(s)

REQ-R180S-GO-1: The RETS Reply Code “0” from the RETS server is necessary for compliance.

3.4.4 Certification Details: Logout Test(s)

REQ-R180S-LO-1: The RETS Reply Code “0” from the RETS server is necessary for compliance.

3.4.5 Certification Details: Search Test(s)

REQ-R180S-S-1: The RETS Reply Code “0” from the RETS server is necessary for compliance.

> **Note:** The RETS Reply Code “20206” from the RETS server signifies an invalid query syntax. This will case the RETS Client to fail this test. See section 7.6 of the RETS 1.8 specification for details.

3.4.6 Certification Details: Update Test(s)

> **NOTE:** Update Functionality is not included in current server certifications.

3.4.7 Certification Details: Metadata Test(s)

REQ-R180S-GM-1: The RETS Reply Code “0” from the RETS server is necessary for compliance.

3.4.8 Certification Details: PostObject

> **NOTE:** PostObject Functionality is not included in current server certifications.

3.4.9 Certification Details: GetPayloadList Test(s)

REQ-R180S -GPL-1: The RETS Reply Code “0” from the RETS server is necessary for compliance.

3.4.10 Non-Certified Functionality

The following RETS 1.8 Server functionality will be ignored for Certification: ChangePassword (Section 9); Update (Section 10); PostObject (Section 13); GetPayloadList (Section 14)

DEFERRED: DMQL2 Time Zone Offsets (7.6.2); DMQL2 “.EMPTY.” session information token

4 RETS 1.x Report Cards

The RETS 1.x Report Cards are used to report to the applicant the certification findings.

The structure of the Report Card is based on the layout of the current RESO Client Test Summary. Final format is to be determined by the Certification Department.