



RESO Web API Server Testing Rules v1.0.3

1.0 Introduction	3
1.1 Glossary	4
1.2 RESO Certification Flow (Summary)	4
2.0 RESO Web API Compliance Rules	5
2.1 RESO Web API Server Compliance Testing Rules	6
2.1.1 Non-RESO Technology Standards included in RESO Web API Compliance Testing Rules	6
2.1.1.1 OData 4.0 OASIS Standard	6
2.1.1.2 OpenID Connect Standard	15
2.1.2 URLs & Endpoint Support	21
2.1.3 Query Support	21
2.1.4 RESO Data Dictionary Support	24
2.1.5 Response Code Support	24
2.1.6 Property Facet Support	25
3.0 RESO Web API Certification Rules	26
3.1 Compliance Levels Definition Summary	27
3.2 RESO Web API Server Certification Level Testing Rules	27
3.2.1 RESO Web API Server Core Certification (Minimum)	28
3.2.2 RESO Web API Server Bronze Certification (Parity)	28
3.2.3 RESO Web API Server Silver Certification (Advanced)	28
3.2.4 RESO Web API Server Gold Certification (Complete)	28
3.2.5 RESO Web API Server Platinum Certification (Maximum)	28
4.0 RESO Web API Report Card and Specifications	29
Change Log	30

RESO Web API Server Testing Rules v1.0.3

Copyright 2015 RESO - All readers of this document must accept RESO End User License Agreement (EULA) posted [here](#).

Date of Last Update: December 5, 2017

1.0 Introduction

- 1.1 Glossary
- 1.2 RESO Certification Flow (Summary)

2.0 RESO Web API Compliance Rules

- 2.1 RESO Web API Server Compliance Testing Rules
 - 2.1.1 Non-RESO Technology Standards included in RESO Web API Compliance Testing Rules
 - 2.1.1.1 OData 4.0 OASIS Standard
 - 2.1.1.1.1 OData 4.0 OASIS Standard: Conformance Rules
 - 2.1.1.1.2 OData 4.0 OASIS Standard: Service Implementation Rules
 - 2.1.1.2 OpenID Connect Standard
 - 2.1.1.2.1 OpenID Certification OP Tests
 - 2.1.2 URLs & Endpoint Support
 - 2.1.3 Query Support
 - 2.1.4 RESO Data Dictionary Support
 - 2.1.5 Response Code Support
 - 2.1.6 Property Facet Support

3.0 RESO Web API Certification Rules

- 3.1 Compliance Levels Definition Summary
- 3.2 RESO Web API Server Certification Level Testing Rules
 - 3.2.1 RESO Web API Server Core Certification (Minimum)
 - 3.2.2 RESO Web API Server Bronze Certification (Parity)
 - 3.2.3 RESO Web API Server Silver Certification (Advanced)
 - 3.2.4 RESO Web API Server Gold Certification (Complete)
 - 3.2.5 RESO Web API Server Platinum Certification (Maximum)

4.0 RESO Web API Report Card and Specifications

Change Log

1.0 Introduction

This document contains the RESO Web API Testing Rules for Servers and Clients.

This document should be read by any organization who wants:

- To create a RESO Web API compliant server or client.
- To gain an understanding of the certification process.

Any organization that wants their implementation certified against the RESO Web API standard follow a multi-step certification process that begins with an application submitted through <http://reso.org/certification>. There are two paths to certification: client or server. Certification as a server shows that the server can deliver structured information. Certification as a client shows that the client can consume structured information. Client and server certification are separate. Organizations that have both a client and a server implementation must complete two certification processes, one for each type.

This document describes the steps and compliance rules that must be satisfied to become certified against the [RESO Web API v1.0.2](#) standard.

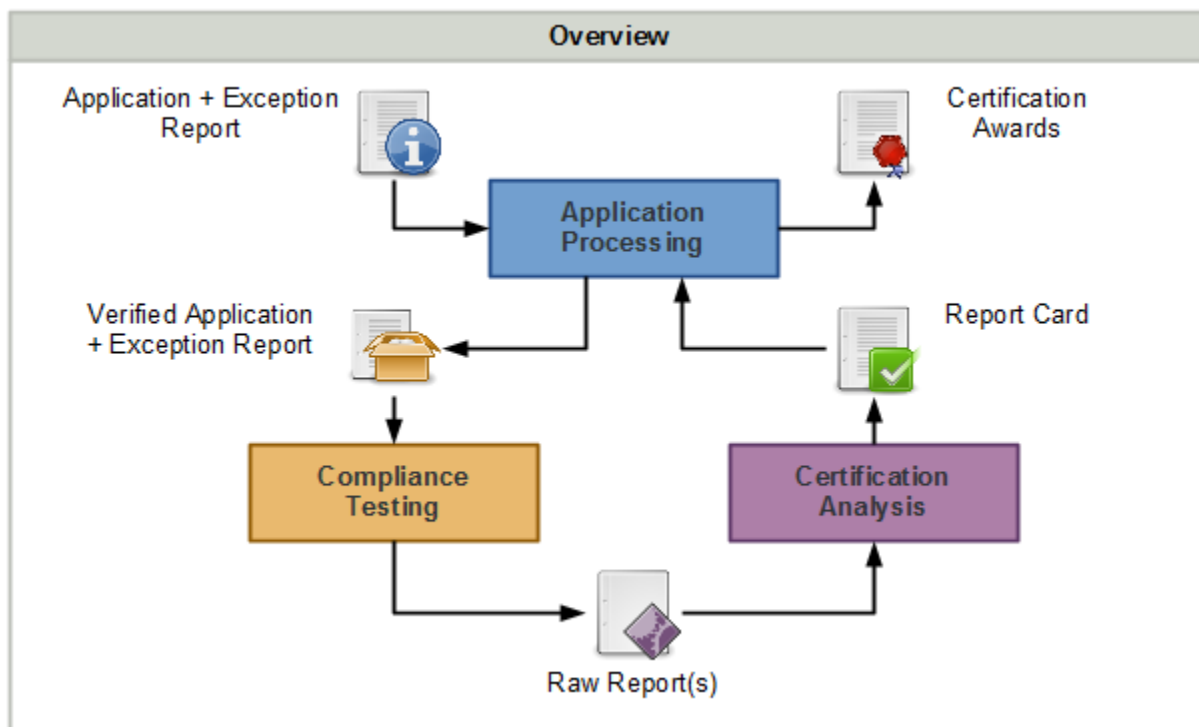
1.1 Glossary

1.2 RESO Certification Flow (Summary)

1.1 Glossary

A glossary for common terms for RESO Web API processes is here <Document TBD>.

1.2 RESO Certification Flow (Summary)



RESO Group	Action	Output
Application Processing (Pre-Certification)	Accept and Verify Applicant's ' Certification Application ' via reso.org/certification	Prepare for Compliance Testing. Pass application and any information provided by applicant to Compliance Department.

Compliance Testing	Test applicant's implementation against well-defined Compliance Rules as set forth by the Transport and Compliance Workgroups.	Testing results formatted in 'Raw Report' package. Pass 'Raw Report' to Certification Department.
Certification Analysis	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.
Application Processing (Post-Certification)	Act on Certification Department recommendation ("Certify" or "Request Changes")	Notify applicant of Certificate Pass/Fail. Send notification and 'Report Card' back to Applicant.

Application Processing (Pre-Certification)

2.0 RESO Web API Compliance Rules

This section contains 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](#).

This version of the RESO Web API Testing Rules will only contain those applying to Web API Servers. The Web API Client Testing Rules will be recorded in a separate document and merged when both are finalized and approved.

2.1 RESO Web API Server Compliance Testing Rules

2.1 RESO Web API Server Compliance Testing Rules

2.1.1 Non-RESO Technology Standards included in RESO Web API Compliance Testing Rules

- 2.1.1.1 OData 4.0 OASIS Standard
 - 2.1.1.1.1 OData 4.0 OASIS Standard: Conformance Rules
 - 2.1.1.1.2 OData 4.0 OASIS Standard: Service Implementation Rules
- 2.1.1.2 OpenID Connect Standard
 - 2.1.1.2.1 OpenID Certification OP Tests

2.1.2 URLs & Endpoint Support

2.1.3 Query Support

2.1.4 RESO Data Dictionary Support

2.1.5 Response Code Support

2.1.6 Property Facet Support

2.1.1 Non-RESO Technology Standards included in RESO Web API Compliance Testing Rules

The RESO Web API standard incorporates external standards from the W3C, OASIS, and the OpenID Foundation.

The RESO Web API is a more restrictive implementation of the external standards without extending into new functionality. The compliance requirements take selected portions of an external standard and make those portions a **MUST** (or **MUST NOT**) requirement where they are a **MAY** (or **MAY NOT**) by the other. Other portions were changed to **"MUST NOT"** where required. Where RESO has not changed the public standard, the certification uses a sub-set of well-defined external test systems.

2.1.1.1 OData 4.0 OASIS Standard

- 2.1.1.1.1 OData 4.0 OASIS Standard: Conformance Rules
- 2.1.1.1.2 OData 4.0 OASIS Standard: Service Implementation Rules

2.1.1.2 OpenID Connect Standard

- 2.1.1.2.1 OpenID Certification OP Tests

2.1.1.1 OData 4.0 OASIS Standard

A server service end point MUST pass the OData 4.0 validation test for either AtomPub/XML or JSON with a Requirement Level of "MUST."

Once this test is completed, the test result is submitted to RESO as part of the certification process.

REQ-WA103-OASIS1: Satisfy OData 4.0 Standards for read-only transactions.

NOTE: The focus here is on passing the basic validation checks for OData 4.0 using the OASIS validation tool here - <http://services.odata.org/validation/validation.htm>

Any server service must first pass these validation checks. Testing is at a read-only, or "minimal" conformance level and metadata.

The exact tests are provided by the OData standard "List of Rules" table for all "MUST" RequirementLevels: <http://services.odata.org/validation/roadmap.htm#rules>

OData Overview^[2]

The Open Data Protocol (OData) is an application-level protocol for interacting with data via RESTful web services. The protocol supports the description of data models and the editing and querying of data according to those models. It provides facilities for:

- Metadata: a machine-readable description of the data model exposed by a particular data provider.
- Data: sets of data entities and the relationships between them.
- Querying: requesting that the service perform a set of filtering and other transformations to its data, then return the results.
- Editing: creating, updating, and deleting data.
- Operations: invoking custom logic.
- Vocabularies: attaching custom semantics.

The OData Protocol provides a uniform way to describe both the data and the data model. This improves semantic interoperability between systems and allows an ecosystem to emerge.

Further details pertaining to OData may be found here: [OData Version 4.0](#)

^[2] Source: © Copyright OASIS Open 2013.

2.1.1.1.1 OData 4.0 OASIS Standard: Conformance Rules

2.1.1.1.2 OData 4.0 OASIS Standard: Service Implementation Rules

2.1.1.1.1 OData 4.0 OASIS Standard: Conformance Rules

The following table contains the OData 4.0 OASIS Standard Conformance Rules as they are applied to the RESO Web API Standard.

NOTE 1-1: All OData Rules are included even if they are NOT required by RESO Testing Rules.

NOTE 1-2: The RESO Web API Testing Tool determines which tests will be applied to the applicant's server. Only those tests applicable for the server being tested will be used to determine compliance.

REQ-WA103-ODATA-CR01: All Conformance Rules results are acceptable for RESO Compliance with the following exception: **ERROR**. **SUCCESS** is recommended result for all tests. The **ABORTED**, **PENDING**, **SKIP**, and **WARNING**, results are acceptable.

NOTE 1-3: This testing rule **MAY** be superseded by any individual rule below. There **MAY** be individual cases where the acceptable results are changed. Review "RESO Compliance Notes" column for additional information.

Table Legend:

- **RESO Rule ID:** A unique rule identifier.
- **OData Rule ID:** The rule identifier provided by the OData Compliance tester.

NOTE 1-4: The rule identifiers are based on the code folder found in the OData ValidationTool on GitHub: https://github.com/OData/ValidationTool/tree/master/test/Data/Conformance_Data

- **OData Description:** A description of the test as provided by the OData Compliance testers.
- **RESO Compliance Level:** Each RESO Rule is assigned to a different compliance level. Systems **MUST** successfully pass ALL of the rules in a compliance level to receive that level. The levels are: CORE, BRONZE, SILVER, GOLD, PLATINUM. The **NONE** Compliance Level is reserved for OData Rules that are NOT required for any level of implementation. The **UNDETERMINED** Compliance Level are those rules that have **NOT** been defined by the RESO Transport Workgroup. Certification applicants will **NOT** be required to pass the rules with **NONE** and **UNDETERMINED** compliance levels.
- **RESO Compliance Notes:** Any additional notes required to understand compliance testing procedures.

RESO Rule ID	OData Rule ID	OData Description	RESO Compliance Level	RESO Compliance Notes
REQ-WA103-ODATA-MinC1001	Minimal.Conformance.1001	1. MUST publish a service document at the service root (section 11.1.1)	Core	Replaces REQ-WA103-END1
REQ-WA103-ODATA-MinC1002	Minimal.Conformance.1002	2. MUST return data according to at least one of the OData defined formats (section 7)	Core	
REQ-WA103-ODATA-MinC1003	Minimal.Conformance.1003	3. MUST support server-driven paging when returning partial results (section 11.2.5.7)	Core	
REQ-WA103-ODATA-MinC1004	Minimal.Conformance.1004	4. MUST return the appropriate OData-Version header (section 8.1.5)	Core	Replaces REQ-WA103-URL1

REQ-WA103-ODATA-MinC1005	Minimal.Conformance.1005	5. MUST conform to the semantics the following headers	Core	
REQ-WA103-ODATA-MinC100501	Minimal.Conformance.100501	5.1. Accept (section 8.2.1)	Core	NOTE MinC100501-01: A server MAY return HTTP 415 (<i>UnsupportedMediaType</i>) when "Accept-Charset:utf-16" is used for servers that only support "utf-8". (Returning 415 may cause the tool to report an error, but this will be ignored for certification testing.)
REQ-WA103-ODATA-MinC100502	Minimal.Conformance.100502	5.2. OData-MaxVersion (section 8.2.7)	Core	
REQ-WA103-ODATA-MinC1006	Minimal.Conformance.1006	6. MUST follow OData guidelines for extensibility (section 6 and all subsections)	Core	
REQ-WA103-ODATA-MinC100603	Minimal.Conformance.100603	1). Services SHOULD fail any request that contains query options that they not understand.(section 6.1)	Core	
REQ-WA103-ODATA-MinC100611	Minimal.Conformance.100611	2). An OData service MUST fail any request that contains actions or functions that it does not understand.	Core	
REQ-WA103-ODATA-MinC1007	Minimal.Conformance.1007	7. MUST successfully parse the request according to [OData-ABNF] for any supported system query string options and either follow the specification or return 501 Not Implemented (section 9.3.1) for any unsupported functionality (section 11.2.1).	Core	
REQ-WA103-ODATA-MinC1008	Minimal.Conformance.1008	8. MUST expose only data types defined in [OData-CSDL]	Core	
REQ-WA103-ODATA-MinC1009	Minimal.Conformance.1009	9. MUST NOT require clients to understand any metadata or instance annotations (section 6.4)	Core	
REQ-WA103-ODATA-MinC1010	Minimal.Conformance.1010	10. MUST NOT violate any OData update semantics (section 11.4 and all subsections).	Core	
REQ-WA103-ODATA-MinC1011	Minimal.Conformance.1011	11. MUST NOT violate any other OData-defined semantics.	Core	
REQ-WA103-ODATA-MinC1012	Minimal.Conformance.1012	12. SHOULD support \$expand (section 11.2.4.2) NOTE: Superseded by REQ-WA103-ODATA-AdvC1009 which converts this rule to MUST for the specified compliance level	Platinum	Replaces REQ-WA103-QO29
REQ-WA103-ODATA-MinC1013	Minimal.Conformance.1013	13. MUST publish metadata at \$metadata according to [OData-CSDL] (section 11.1.2)	Core	Replaces REQ-WA103-END3 (RESO changed MAY to MUST)
RESO Rule ID	OData Rule ID	OData Description	RESO Compliance Level	RESO Compliance Notes

REQ-WA103-ODATA-IntC1001	Intermediate.Conformance.1001	1. MUST conform to the OData Minimal Conformance Level.	n/a	This summary requirement of all " REQ-WA103-ODATA-MinC#### " rules. No specific test associated with this requirement.
REQ-WA103-ODATA-IntC1002	Intermediate.Conformance.1002	2. MUST successfully parse the [OData-ABNF] and either follow the specification or return 501 Not Implemented for any unsupported functionality (section 9.3.1).	Bronze	
REQ-WA103-ODATA-IntC1003	Intermediate.Conformance.1003	3. MUST support \$select (section 11.2.4.1)	Core	Replaces REQ-WA103-QR3
REQ-WA103-ODATA-IntC1005	Intermediate.Conformance.1005	5. MUST support \$top (section 11.2.5.3)	Core	Replaces REQ-WA103-QR4
REQ-WA103-ODATA-IntC1006	Intermediate.Conformance.1006	6. MUST support \$value on media entities (section 4.10. in [OData-URL]) and individual properties (section 11.2.3.1)	Platinum	
REQ-WA103-ODATA-IntC1007	Intermediate.Conformance.1007	7. MUST support \$filter (section 11.2.5.1)	Core	Replaces REQ-WA103-QO1
REQ-WA103-ODATA-IntC100701	Intermediate.Conformance.100701	7.1. MUST support eq	Core	Replaces REQ-WA103-QO2
REQ-WA103-ODATA-IntC100702	Intermediate.Conformance.100702	7.2. MUST support aliases in \$filter expressions (section 11.2.5.1.3)	Platinum	
REQ-WA103-ODATA-IntC100703	Intermediate.Conformance.100703	7.3. SHOULD support additional filter operations (section 11.2.5.1.1) and MUST return 501 Not Implemented for any unsupported filter operations (section 9.3.1)	Bronze	
REQ-WA103-ODATA-IntC100704	Intermediate.Conformance.100704	7.4. SHOULD support the canonical functions (section 11.2.5.1.2) and MUST return 501 Not Implemented for any unsupported canonical functions (section 9.3.1)	Bronze	
REQ-WA103-ODATA-IntC100705	Intermediate.Conformance.100705	7.5. SHOULD support \$filter on expanded entities (section 11.2.4.2.1) <i>NOTE: Superseded by REQ-WA103-ODATA-AdvC1009 which converts this rule to MUST for the specified compliance level</i>	Platinum	Replaces REQ-WA103-QO29
REQ-WA103-ODATA-IntC1008	Intermediate.Conformance.1008	8. SHOULD publish metadata at \$metadata according to [OData-CSDL] (section 11.1.2)	Bronze	
REQ-WA103-ODATA-IntC1009	Intermediate.Conformance.1009	9. SHOULD support the [OData-JSON] format.	Bronze	
REQ-WA103-ODATA-IntC1010	Intermediate.Conformance.1010	10. SHOULD consider supporting basic authentication as specified in [RFC2617] over HTTPS for the highest level of interoperability with generic clients.	Not Tested	OpenID is the RESO authentication standard.
REQ-WA103-ODATA-IntC1011	Intermediate.Conformance.1011	11. SHOULD support the \$search system query option (section 11.2.5.6)	Platinum	

REQ-WA103-ODATA-IntC1012	Intermediate.Conformance.1012	12. SHOULD support the \$skip system query option (section 11.2.5.4) NOTE: Superseded by REQ-WA103-ODATA-AdvC1006 which converts this rule to MUST for the specified compliance level	Core	Replaces REQ-WA103-QR5
REQ-WA103-ODATA-IntC1014	Intermediate.Conformance.1014	14. SHOULD support \$expand (section 11.2.4.2) NOTE: Superseded by REQ-WA103-ODATA-AdvC1009 which converts this rule to MUST for the specified compliance level	Platinum	Replaces REQ-WA103-QO29
REQ-WA103-ODATA-IntC1017	Intermediate.Conformance.1017	17. SHOULD support \$orderby asc and desc on individual properties (section 11.2.5.2) NOTE: Superseded by REQ-WA103-ODATA-AdvC1008 which converts this rule to MUST for the specified compliance level	Bronze	Replaces REQ-WA103-QO28
RESO Rule ID	OData Rule ID	OData Description	RESO Compliance Level	RESO Compliance Notes
REQ-WA103-ODATA-AdvC1001	Advanced.Conformance.1001	1. MUST conform to at least the OData Intermediate Conformance Level.	n/a	This summary requirement of all " REQ-WA103-ODATA-IntC#### " rules. No specific test associated with this requirement.
REQ-WA103-ODATA-AdvC1002	Advanced.Conformance.1002	2. MUST publish metadata at \$metadata according to [OData-CSDL] (section 11.1.2)	Bronze	
REQ-WA103-ODATA-AdvC1003	Advanced.Conformance.1003	3. MUST support the [OData-JSON] format.	Bronze	
REQ-WA103-ODATA-AdvC1006	Advanced.Conformance.1006	6. MUST support the \$skip system query option (section 11.2.5.4)	Core	Replaces REQ-WA103-QR5
REQ-WA103-ODATA-AdvC1008	Advanced.Conformance.1008	8. MUST support \$orderby asc and desc on individual properties (section 11.2.5.2)	Bronze	Replaces REQ-WA103-QO28
REQ-WA103-ODATA-AdvC1009	Advanced.Conformance.1009	9. MUST support \$expand (section 11.2.4.2)	Platinum	Replaces REQ-WA103-QO29
REQ-WA103-ODATA-AdvC100901	Advanced.Conformance.100901	9.1. MUST support returning references for expanded properties (section 11.2.4.2)	Platinum	Replaces REQ-WA103-QO29
REQ-WA103-ODATA-AdvC100902	Advanced.Conformance.100902	9.2. MUST support \$filter on expanded entities (section 11.2.4.2.1)	Platinum	
REQ-WA103-ODATA-AdvC100904	Advanced.Conformance.100904	9.4. SHOULD support \$orderby asc and desc on individual properties (section 11.2.4.2.1) NOTE: Superseded by REQ-WA103-ODATA-AdvC1008 which converts this rule to MUST for the specified compliance level	Bronze	Replaces REQ-WA103-QO28
REQ-WA103-ODATA-AdvC100905	Advanced.Conformance.100905	9.5. SHOULD support the \$count system query option for expanded properties (section 11.2.4.2.1)	Platinum	

REQ-WA103-ODATA-AdvC100906	Advanced.Conformance.100906	9.6. SHOULD support \$top and \$skip on expanded properties (section 11.2.4.2.1)	Platinum	
REQ-WA103-ODATA-AdvC100907	Advanced.Conformance.100907	9.7. SHOULD support \$search on expanded properties (section 11.2.4.2.1)	Platinum	
REQ-WA103-ODATA-AdvC100908	Advanced.Conformance.100908	9.8. SHOULD support \$levels for recursive expand (section 11.2.4.2.1.1)	Platinum	
REQ-WA103-ODATA-AdvC1010	Advanced.Conformance.1010	10. MUST support the \$search system query option (section 11.2.5.6)	Platinum	
REQ-WA103-ODATA-AdvC1011	Advanced.Conformance.1011	11. MUST support batch requests (section 11.7 and all subsections)	Platinum	
REQ-WA103-ODATA-AdvC101101	Advanced.Conformance.101101	1). Services MUST support all three formats: Absolute URI with schema, host, port, and absolute resource path.	Core	Replaces REQ-WA103-URL2 & REQ-WA103-URL3 (TBD)
REQ-WA103-ODATA-AdvC101102	Advanced.Conformance.101102	2). A service MUST process the components of the Batch in the order received. (section 11.7.4)	Platinum	
REQ-WA103-ODATA-AdvC101106	Advanced.Conformance.101106	4). The service MUST include the Content-ID header in each response with the same value that the client specified in the corresponding request. (section 11.7.4)	Bronze	
REQ-WA103-ODATA-AdvC101107	Advanced.Conformance.101107	5). If the set of request headers of a Batch request are valid the service MUST return a 200 OK HTTP response code. (section 11.7.4)	Platinum	
REQ-WA103-ODATA-AdvC101108	Advanced.Conformance.101108	6). If the service receives a Batch request with an invalid set of headers it MUST return a 4xx response code. (section 11.7.4)	Platinum	
REQ-WA103-ODATA-AdvC101109	Advanced.Conformance.101109	7). A response to a batch request MUST contain a Content-Type header with value multipart/mixed. (section 11.7.4)	Platinum	
REQ-WA103-ODATA-AdvC101110	Advanced.Conformance.101110	8). Structurally, a batch response body MUST match one-to-one with the corresponding batch request body. (section 11.7.4)	Platinum	
REQ-WA103-ODATA-AdvC101111	Advanced.Conformance.101111	9). When a request within a change set fails, the change set response is represented using the application/http media type and a Content-Transfer-Encoding header with a value of binary instead of using the multipart/mixed media type. (section 11.7.4)	Platinum	
REQ-WA103-ODATA-AdvC101117	Advanced.Conformance.101117	10). When an error occurs processing a request and the odata.continue-on-error preference is not specified, processing of the batch is terminated and the error response is the last part of the multi-part response. (section 11.7.4)	Platinum	

REQ-WA103-ODATA-AdvC1012	Advanced.Conformance.1012	12. MUST support the resource path conventions defined in [OData-URL]	Platinum	
REQ-WA103-ODATA-AdvC1013	Advanced.Conformance.1013	13. SHOULD support Asynchronous operations.	Platinum	
REQ-WA103-ODATA-AdvC1014	Advanced.Conformance.1014	14. SHOULD support Delta change tracking.	Platinum	
REQ-WA103-ODATA-AdvC1015	Advanced.Conformance.1015	15. SHOULD support cross-join queries defined in [OData-URL].	Platinum	
REQ-WA103-ODATA-AdvC1016	Advanced.Conformance.1016	16. SHOULD support a conforming OData service interface over metadata.	Platinum	

2.1.1.1.2 OData 4.0 OASIS Standard: Service Implementation Rules

The following table contains the OData 4.0 OASIS Standard Service Implementation Rules as they are applied to the RESO Web API Standard.

NOTE 1-1: All OData Rules are included even if they are NOT required by RESO Testing Rules.

NOTE 1-2: The RESO Web API Testing Tool determines which tests will be applied to the applicant's server. Only those tests applicable for the server being tested will be used to determine compliance.

REQ-WA103-ODATA-SIR01: All Conformance Rules results are acceptable for RESO Compliance with the following exception: **ERROR**. **SUCCESS** is recommended result for all tests. The **ABORTED**, **PENDING**, **SKIP**, and **WARNING**, results are acceptable.

NOTE 1-3: This testing rule **MAY** be superseded by any individual rule below. There **MAY** be individual cases where the acceptable results are changed. Review "RESO Compliance Notes" column for additional information.

Table Legend:

- **RESO Rule ID:** A unique rule identifier.
- **OData Rule ID:** The rule identifier provided by the OData Compliance tester.

NOTE 1-4: The rule identifiers are based on the file names found in the OData ValidationTool on GitHub: <https://github.com/ODa/ta/ValidationTool/tree/master/src/CodeRules/ServiceImplementation>

- **OData Description:** A description of the test as provided by the OData Compliance testers.
- **RESO Compliance Level:** Each RESO Rule is assigned to a different compliance level. Systems **MUST** successfully pass ALL of the rules in a compliance level to receive that level. The levels are: CORE, BRONZE, SILVER, GOLD, PLATINUM. The **NONE** Compliance Level is reserved for OData Rules that are NOT required for any level of implementation. The **UNDETERMINED** Compliance Level are those rules that have **NOT** been defined by the RESO Transport Workgroup. Certification applicants will **NOT** be required to pass the rules with **NONE** and **UNDETERMINED** compliance levels.
- **RESO Compliance Notes:** Any additional notes required to understand compliance testing procedures.

RESO Rule ID	OData Rule ID	OData Description	RESO Compliance Level	RESO Compliance Notes
REQ-WA103-ODATA-SI-BR	ServiceImpl_BatchRequests	Batch Requests,Batch Requests	Platinum	
REQ-WA103-ODATA-SI-AR	ServiceImpl_AsynchronousRequest	Asynchronous Requests,Asynchronous Requests	Platinum	
REQ-WA103-ODATA-SI-AIM	ServiceImpl_ActionImport	Operations,ActionImport	Platinum	
REQ-WA103-ODATA-SI-CJ	ServiceImpl_CrossJoin	Requesting Data,Cross Join	Platinum	
REQ-WA103-ODATA-SI-E	ServiceImpl_Etag	Response Headers,Etag	Platinum	
REQ-WA103-ODATA-SI-FG	ServiceImpl_FilterGrouping	Requesting Data,System Query Option,Logical Operators,\$filter (Grouping)	Platinum	Replaces REQ-WA103-QO12
REQ-WA103-ODATA-SI-FH	ServiceImpl_FilterHas	Requesting Data,System Query Option,Logical Operators,\$filter (Has)	Bronze	Replaces REQ-WA103-QO8
REQ-WA103-ODATA-SI-FN	ServiceImpl_FilterNot	Requesting Data,System Query Option,Logical Operators,\$filter (Not)	Core	Replaces REQ-WA103-QO11

REQ-WA103-ODATA-SI-SQ OFCA	ServiceImpl_SystemQueryOptionFilter_Cast	Requesting Data, System Query Option, Arithmetic Operators, \$filter(cast)	Platinum	
REQ-WA103-ODATA-SI-SQ OFCE	ServiceImpl_SystemQueryOptionFilter_Ceiling	Requesting Data, System Query Option, Arithmetic Operators, \$filter(ceiling)	Platinum	
REQ-WA103-ODATA-SI-SQ OFCC	ServiceImpl_SystemQueryOptionFilter_Concat	Requesting Data, System Query Option, Arithmetic Operators, \$filter(concat)	Platinum	
REQ-WA103-ODATA-SI-SQ OFCT	ServiceImpl_SystemQueryOptionFilter_Contains	Requesting Data, System Query Option, Arithmetic Operators, \$filter(contains)	Platinum	Replaces REQ-WA103-QO13
REQ-WA103-ODATA-SI-SQ OFDAY	ServiceImpl_SystemQueryOptionFilter_Day	Requesting Data, System Query Option, Arithmetic Operators, \$filter(day)	Gold	Replaces REQ-WA103-QO20
REQ-WA103-ODATA-SI-SQ OFDIV	ServiceImpl_SystemQueryOptionFilter_Division	Requesting Data, System Query Option, Arithmetic Operators, \$filter(Division)	Platinum	
REQ-WA103-ODATA-SI-SQ OFEW	ServiceImpl_SystemQueryOptionFilter_EndsWith	Requesting Data, System Query Option, Arithmetic Operators, \$filter(endswith)	Platinum	Replaces REQ-WA103-QO14
REQ-WA103-ODATA-SI-SQ OFF	ServiceImpl_SystemQueryOptionFilter_Floor	Requesting Data, System Query Option, Arithmetic Operators, \$filter(floor)	Platinum	
REQ-WA103-ODATA-SI-SQ OFFS	ServiceImpl_SystemQueryOptionFilter_Fractionalseconds	Requesting Data, System Query Option, Arithmetic Operators, \$filter(fractionalseconds)	Gold	Replaces REQ-WA103-QO24
REQ-WA103-ODATA-SI-SQ OFH	ServiceImpl_SystemQueryOptionFilter_Hour	Requesting Data, System Query Option, Arithmetic Operators, \$filter(hour)	Gold	Replaces REQ-WA103-QO21
REQ-WA103-ODATA-SI-SQ OFIN	ServiceImpl_SystemQueryOptionFilter_IndexOf	Requesting Data, System Query Option, Arithmetic Operators, \$filter(indexof)	Platinum	
REQ-WA103-ODATA-SI-SQ OFIS	ServiceImpl_SystemQueryOptionFilter_IsOf	Requesting Data, System Query Option, Arithmetic Operators, \$filter(isof)	Platinum	
REQ-WA103-ODATA-SI-SQ OFL	ServiceImpl_SystemQueryOptionFilter_Length	Requesting Data, System Query Option, Arithmetic Operators, \$filter(length)	Platinum	
REQ-WA103-ODATA-SI-SQ OFMAXDT	ServiceImpl_SystemQueryOptionFilter_Maxdatetime	Requesting Data, System Query Option, Arithmetic Operators, \$filter(maxdatetime)	Platinum	
REQ-WA103-ODATA-SI-SQ OFMINDT	ServiceImpl_SystemQueryOptionFilter_Mindatetime	Requesting Data, System Query Option, Arithmetic Operators, \$filter(mindatetime)	Platinum	
REQ-WA103-ODATA-SI-SQ OFMIN	ServiceImpl_SystemQueryOptionFilter_Minute	Requesting Data, System Query Option, Arithmetic Operators, \$filter(minute)	Gold	Replaces REQ-WA103-QO22
REQ-WA103-ODATA-SI-SQ OFMOD	ServiceImpl_SystemQueryOptionFilter_Modulo	Requesting Data, System Query Option, Arithmetic Operators, \$filter(Modulo)	Platinum	
REQ-WA103-ODATA-SI-SQ OFMON	ServiceImpl_SystemQueryOptionFilter_Month	Requesting Data, System Query Option, Arithmetic Operators, \$filter(month)	Gold	Replaces REQ-WA103-QO19
REQ-WA103-ODATA-SI-SQ OFMULT	ServiceImpl_SystemQueryOptionFilter_Multiplication	Requesting Data, System Query Option, Arithmetic Operators, \$filter(Multiplication)	Platinum	
REQ-WA103-ODATA-SI-SQ OFNEG	ServiceImpl_SystemQueryOptionFilter_Negation	Requesting Data, System Query Option, Arithmetic Operators, \$filter(Negation)	Platinum	

REQ-WA103-ODATA-SI-SQ OFNOW	ServiceImpl_SystemQueryOptionFilter_Now	Requesting Data, System Query Option, Arithmetic Operators, \$filter(now)	Core	Replaces REQ-WA103-QO27
REQ-WA103-ODATA-SI-SQ OFR	ServiceImpl_SystemQueryOptionFilter_Round	Requesting Data, System Query Option, Arithmetic Operators, \$filter(round)	Undetermined	
REQ-WA103-ODATA-SI-SQ OFSEC	ServiceImpl_SystemQueryOptionFilter_Second	Requesting Data, System Query Option, Arithmetic Operators, \$filter(second)	Gold	Replaces REQ-WA103-QO23
REQ-WA103-ODATA-SI-SQ OFSW	ServiceImpl_SystemQueryOptionFilter_StartsWith	Requesting Data, System Query Option, Arithmetic Operators, \$filter(startswith)	Platinum	Replaces REQ-WA103-QO15
REQ-WA103-ODATA-SI-SQ OFS	ServiceImpl_SystemQueryOptionFilter_Substring	Requesting Data, System Query Option, Arithmetic Operators, \$filter(substring)	Platinum	
REQ-WA103-ODATA-SI-SQ OFTL	ServiceImpl_SystemQueryOptionFilter_ToLower	Requesting Data, System Query Option, Arithmetic Operators, \$filter(tolower)	Platinum	Replaces REQ-WA103-QO16
REQ-WA103-ODATA-SI-SQ OFTS	ServiceImpl_SystemQueryOptionFilter_TotalSeconds	Requesting Data, System Query Option, Arithmetic Operators, \$filter(totalseconds)	Platinum	
REQ-WA103-ODATA-SI-SQ OFTU	ServiceImpl_SystemQueryOptionFilter_ToUpper	Requesting Data, System Query Option, Arithmetic Operators, \$filter(toupper)	Platinum	Replaces REQ-WA103-QO17
REQ-WA103-ODATA-SI-SQ OFTRIM	ServiceImpl_SystemQueryOptionFilter_Trim	Requesting Data, System Query Option, Arithmetic Operators, \$filter(trim)	Platinum	
REQ-WA103-ODATA-SI-SQ OFY	ServiceImpl_SystemQueryOptionFilter_Year	Requesting Data, System Query Option, Arithmetic Operators, \$filter(year)	Gold	Replaces REQ-WA103-QO18
REQ-WA103-ODATA-SI-SQ OEId	ServiceImpl_SystemQueryOptionEntity_Id	Requesting Data, System Query Option, \$entity(\$id)	Platinum	
REQ-WA103-ODATA-SI-SQ OE	ServiceImpl_SystemQueryOptionExpand	Requesting Data, System Query Option, \$expand	Platinum	Replaces REQ-WA103-QO29
REQ-WA103-ODATA-SI-SQ OF	ServiceImpl_SystemQueryOptionFilter	Requesting Data, System Query Option, \$filter	Platinum	
REQ-WA103-ODATA-SI-SQ OFA	ServiceImpl_SystemQueryOptionFilter_Addition	Requesting Data, System Query Option, Arithmetic Operators, \$filter(Addition)	Platinum	
REQ-WA103-ODATA-SI-SQ OFSUB	ServiceImpl_SystemQueryOptionFilter_Subtraction	Requesting Data, System Query Option, Arithmetic Operators, \$filter(Subtraction)	Platinum	
REQ-WA103-ODATA-SI-SQ OFOR	ServiceImpl_SystemQueryOptionFormat	Requesting Data, System Query Option, \$format	Platinum	
REQ-WA103-ODATA-SI-SQ OOB	ServiceImpl_SystemQueryOptionOrderBy	Requesting Data, System Query Option, \$orderby	Bronze	Replaces REQ-WA103-QO28
REQ-WA103-ODATA-SI-SQ OR	ServiceImpl_SystemQueryOptionRef	Requesting Data, System Query Option, \$ref	Platinum	
REQ-WA103-ODATA-SI-SQ OSH	ServiceImpl_SystemQueryOptionSearch	Requesting Data, System Query Option, \$search	Platinum	
REQ-WA103-ODATA-SI-SQ OST	ServiceImpl_SystemQueryOptionSelect	Requesting Data, System Query Option, \$select	Core	Replaces REQ-WA103-QR3
REQ-WA103-ODATA-SI-SQ OT	ServiceImpl_SystemQueryOptionTop	Requesting Data, System Query Option, \$top	Core	Replaces REQ-WA103-QR4
REQ-WA103-ODATA-SI-SQ OV	ServiceImpl_SystemQueryOptionValue	Requesting Data, System Query Option, \$value	Platinum	

2.1.1.2 OpenID Connect Standard

The [RESO Web API Security](#) Document outlines the security protocols required for RESO Web API Servers. These security protocols focus on

Security Classifications for RESO Web API Server Certificates

REQ-WA103-SC0: Applicants **MUST** satisfy one of the following security classification sets to receive a RESO Web API Certificate:

1. RESO Web API 1.0.3 Server Certification with **OpenID Connect**
2. RESO Web API 1.0.3 Server Certification with **OAuth 2 Bearer Token**
3. RESO Web API 1.0.3 Server Certification with **OAuth 2 Client Credentials**

NOTE SC0-1: It is expected the great majority of applicants will be required to receive the "OpenID Connect" security classification. Applicants who **DO NOT** request a specific security classification will be tested with the "OpenID Connect" rules set. Applicants may request to receive multiple classifications.

REQ-WA103-SC1: The "OpenID Connect" Classification is awarded when **ALL** of the following testing rules are satisfied:

- **REQ-WA103-OPENID1**
- **REQ-WA103-OPENID2**
- **REQ-WA103-BT1**

NOTE SC1-1: This is the classification **REQUIRED** for any Web API server that will be accessed by end users, web browsers, Web API clients that use [Authorization Code Flow](#) of the [OpenID Connect Protocol Suite](#), etc.

NOTE SC1-2: Certification applicants **MAY** use the OpenID Connect Provider Conformance Tests to satisfy the previous requirements: <https://op.certification.openid.net:60000/>.

REQ-WA103-SC2: The "OAuth 2 Bearer Token" Classification is awarded when **ALL** of the following testing rules are satisfied:

- **REQ-WA103-BT1**
- **REQ-WA103-BT2**

NOTE SC2-1: This Certification Classification is for **ONLY** "server-to-server" communications. The applicant's server is not meant for end users. (i.e. no web browser will ever be used for this server.)

REQ-WA103-SC3: The "OAuth 2 Client Credentials" Classification is awarded when **ALL** of the following testing rules are satisfied:

- **REQ-WA103-CC1**

Security Classification Testing Rules

The following requirements come from the [RESO Web API Security Document Section 1 - RESO Security Requirement](#):

REQ-WA103-OPENID1: A compliant RESO Web API Server v1.0.3 **MUST** support [Authorization Code Flow](#) of the [OpenID Connect Protocol Suite](#) as the authentication method for user based communication.

NOTE 1-1: This requirement is waived for applicants who receive one of the "OAuth 2" security classification. Applicants **MUST** request the alternate security classification.

REQ-WA103-OPENID2: A compliant RESO Web API Server v1.0.3 **MAY** use any of the additional [OpenID Connect Protocol Suite](#) of standard specifications.

NOTE 2-1: The additional protocols **ARE NOT** a replacement for the **REQUIRED** [Authorization Code Flow](#).

NOTE 2-2: The additional protocol suite includes: Discovery, Dynamic Client Registration, Session Management, or Form Post Response Mode. (Any newer protocols approved by OpenID Foundation **MUST** be reviewed by RESO Transport Work Group prior to being allowed for this testing rule.)

NOTE 2-3: RESO Transport Testing Tools **WILL NOT** test these optional means of connecting to a server. Certification testing will focus on [Authorization Code Flow](#) only.

REQ-WA103-BT1: A compliant RESO Web API Server v1.0.3 **MUST** support token based authentication with an HTTP Authorization header of "Bearer <token>" where the format of <token> is defined by the compliant RESO Web API Server v1.0.3.

NOTE BT1-1: This is satisfied when the Transport Testing Tool is able access the bearer token and display it within the tool's user interface.

REQ-WA103-BT2: A compliant RESO Web API Server v1.0.3 **MUST** support [Section 2.1 of RFC 6750 OAuth2 Bearer Token Usage](#) as the authentication method for server-to-server based communication.

NOTE BT2-1: These are satisfied when the Transport Testing Tool is able access information on a server with a bearer token, provided by any means, including electronic communication or other physical means.

REQ-WA103-CC1: A compliant RESO Web API Server v1.0.3 **MUST** use the OAuth2 Client Credentials Grant specified in [Section 4.4 of RFC 6749 The OAuth 2.0 Authorization Framework](#).

NOTE CC1-1: This is satisfied when the Transport Testing Tool is able access information on a server using Client Credentials compliant login information, provided by any means, including electronic communication or other physical means.

2.1.1.2.1 OpenID Certification OP Tests

2.1.1.2.1 OpenID Certification OP Tests

Those seeking to receive a "RESO Web API 1.0.3 Server Certification with OpenID Connect" **SHOULD** use the "OpenID Connect Provider Certification" testing tool found at <https://op.certification.openid.net:60000/>. Applicants are encouraged to create and test their own profile on the testing tool before submitting their certification application.

Creating a new "OpenID Connect Provider Certification" Configuration

Applicants creating a new configuration profile will need to provide the following:

1. The "issuer" URL of the server to be tested for certification (without .well-known). Given the discovery endpoint <https://openid.reso.org/.well-known/openid-configuration>, the issuer URL would be <https://openid.reso.org/>
2. The "Features" the server to be tested supports. The options are WebFinger, Dynamic Provider Information Discovery, and Dynamic Client Registration.
3. The one "Response Type" to match the server's configuration. The options are code (Basic), id_token (Implicit), id_token token (Implicit), code id_token (Hybrid), code token (Hybrid), or code id_token token (Hybrid).
4. The optional "tag" may be any value, including default. It is recommended to use RESOCERTIFICATION to allow a unique profile to be created for production certification testing.

REQ-WA103-OPENID-CONFIG1: RESO Web API Servers **MAY** support the WebFinger feature. This feature **WILL NOT** be included in Certification Testing.

REQ-WA103-OPENID-CONFIG2: RESO Web API Servers **MAY** support the Dynamic Provider Information Discovery feature. This feature **WILL BE** included in Certification Testing **IF** supported by the server. The testing rules for this feature are included in the table below. The "OpenID Connect Provider Certification" will determine what tests are required.

REQ-WA103-OPENID-CONFIG3: RESO Web API Servers **MAY** support the Dynamic Client Registration feature. This feature **WILL BE** included in Certification Testing **IF** supported by the server. The testing rules for this feature are included in the table below. The "OpenID Connect Provider Certification" will determine what tests are required.

REQ-WA103-OPENID-CONFIG4: RESO Web API Servers **MUST** support at least **ONE** of any of the Response Types required by the testing tool: **code** (Basic), **id_token** (Implicit), **id_token token** (Implicit), **code id_token** (Hybrid), **code token** (Hybrid), or **code id_token token** (Hybrid). The selection of the Response Type will determine which of the rules in the table below will be required for certification testing. The "OpenID Connect Provider Certification" will determine what tests are required.

Requirements for "OpenID Connect Provider Certification" Testing

The table below contains the RESO Certification Requirements for the tests found within the "OpenID Connect Provider Certification" testing tool.

NOTE 1: The tests presented by the "OpenID Connect Provider Certification" testing tool changes based on the configuration established when the profile is created. RESO **WILL NOT** require additional tests than those presented by the "OpenID Connect Provider Certification" testing tool, assuming that the profile is correctly configured per RESO and OpenID specifications.

NOTE 2: Any tests presented by the "OpenID Connect Provider Certification" testing tool that are **NOT** documented below **WILL NOT** prevent certification. The rule will be reviewed by the applicable RESO Work Groups and included in future Certification Testing Rule documentation. Tests that are considered critical by RESO Work Groups will go into immediate effect.

RESO Rule ID	OpenID Test Category	OpenID Test Name	OpenID Test Description	Required Results	RESO Compliance Level	RESO Compliance Notes
REQ-WA103-OPENID-RTR M1	Response Type & Response Mode	OP-Response-Missing	Authorization request missing the response_type parameter	Success	Core	There are two acceptable outcomes: (1) returning an error response to the RP or (2) returning an error message to the End-User.
REQ-WA103-OPENID-RTR M2	Response Type & Response Mode	OP-Response-code	Request with response_type=code	Success	Core	
REQ-WA103-OPENID-RTR M3	Response Type & Response Mode	OP-Response-id_token	Request with response_type=id_token	Success	Core	

REQ-WA103-OPENID-RTRM4	Response Type & Response Mode	OP-Response-token	Request with response_type=token	Success	Core	
REQ-WA103-OPENID-RTRM5	Response Type & Response Mode	OP-Response-code+id_token+token	Request with response_type=code	Success	Core	
REQ-WA103-OPENID-RTRM6	Response Type & Response Mode	OP-Response-form_post	Request with response_mode=form_post	Not Required	Not Required	
REQ-WA103-OPENID-DISC-CONFIG1	Discovery	OP-Discovery-Config	Publishes openid-configuration discovery information	Success	Core	
REQ-WA103-OPENID-DISC-JWK1	Discovery	OP-Discovery-JWKS	Keys in OP JWKS well formed	Success	Core	
REQ-WA103-OPENID-DISC-JWK2	Discovery	OP-Discovery-jwks_uri	Verify that jwks_uri is published	Success	Core	
REQ-WA103-OPENID-DISC-CLAIM1	Discovery	OP-Discovery-claims_supported	Verify that claims_supported is published	Success	Core	
REQ-WA103-OPENID-ID1	ID Token	OP-IDToken-C-Signature	Does the OP sign the ID Token and with what	Success	Core	
REQ-WA103-OPENID-ID2	ID Token	OP-IDToken-at_hash	ID Token has at_hash when ID Token and Access Token returned from Authorization Endpoint	Success	Core	
REQ-WA103-OPENID-ID3	ID Token	OP-IDToken-c_hash	ID Token has c_hash when ID Token and Authorization Code returned from Authorization Endpoint	Success	Core	
REQ-WA103-OPENID-ID4	ID Token	OP-IDToken-kid	IDToken has kid	Success	Core	
REQ-WA103-OPENID-CA1	Client Authentication	OP-ClientAuth-Basic-Static	Access token request with client_secret_basic authentication	Success	Core	
REQ-WA103-OPENID-CA2	Client Authentication	OP-ClientAuth-SecretPost-Static	Access token request with client_secret_post authentication	Success or Warning	Undetermined	
REQ-WA103-OPENID-AT1	Access Token	OP-Token-refresh	To refresh an Access Token	Not Required	Not Required	
REQ-WA103-OPENID-UEP1	Userinfo Endpoint	OP-UserInfo-Body	UserInfo Endpoint access with POST and bearer body	Success	Core	
REQ-WA103-OPENID-UEP2	Userinfo Endpoint	OP-UserInfo-Endpoint	UserInfo Endpoint access with GET and bearer header	Success	Core	
REQ-WA103-OPENID-UEP3	Userinfo Endpoint	OP-UserInfo-Header	UserInfo Endpoint access with POST and bearer header	Success	Core	
REQ-WA103-OPENID-CRP1	claims Request Parameter	OP-claims-essential	Claims request with essential name claim	Success or Warning	Core	
REQ-WA103-OPENID-DRP1	display Request Parameter	OP-display-page	Request with display=page	Success	Core	
REQ-WA103-OPENID-DRP2	display Request Parameter	OP-display-page	Request with display=popup	Success or Warning	Core	
REQ-WA103-OPENID-NRP1	nonce Request Parameter	OP-nonce-Nonce-req-nocode	Reject requests without nonce unless using the code flow	Success	Core	

REQ-WA103-OPENID-NRP 2	nonce Request Parameter	OP-nonce-nonce	Request with nonce, verifies it was returned in ID Token	Success	Core	
REQ-WA103-OPENID-NRP 3	nonce Request Parameter	OP-nonce-code	ID Token has nonce when requested for code flow	Success	Core	
REQ-WA103-OPENID-PRP 1	prompt Request Parameter	OP-prompt-login	Request with prompt=login	Success	Core	
REQ-WA103-OPENID-PRP 2	prompt Request Parameter	OP-prompt-none-LoggedIn	Request with prompt=none when logged in	Success	Core	
REQ-WA103-OPENID-PRP 3	prompt Request Parameter	OP-prompt-none-NotLoggedIn	Request with prompt=none when not logged in	Success	Core	
REQ-WA103-OPENID-REURP1	redirect_uri Request Parameter	OP-redirect_uri-NotReg	Sent redirect_uri does not match a registered redirect_uri	Success	Core	Displaying an error screen is the required and expected behavior.
REQ-WA103-OPENID-REURP2	redirect_uri Request Parameter	OP-redirect_uri-Missing	Reject request without redirect_uri when multiple registered	Success	Core	
REQ-WA103-OPENID-REURP3	redirect_uri Request Parameter	OP-redirect_uri-Query-Added	Request with redirect_uri with query component when registered redirect_uri has no query component	Success	Core	
REQ-WA103-OPENID-REURP4	redirect_uri Request Parameter	OP-redirect_uri-Query-Mismatch	Rejects redirect_uri when query parameter does not match what is registered	Success	Core	
REQ-WA103-OPENID-REURP5	redirect_uri Request Parameter	OP-redirect_uri-Query-OK	Request with a redirect_uri with a query component when a redirect_uri with the same query component is registered	Success	Core	
REQ-WA103-OPENID-REURP6	redirect_uri Request Parameter	OP-redirect_uri-RegFrag	Reject registration where a redirect_uri has a fragment	Success	Core	
REQ-WA103-OPENID-RQURP1	request_uri Request Parameter	OP-request_uri-Support	Support request_uri request parameter	Success	Core	
REQ-WA103-OPENID-RQURP2	request_uri Request Parameter	OP-request_uri-Unsigned-Dynamic	Support request_uri request parameter with unsigned request	Success	Core	
REQ-WA103-OPENID-RQURP3	request_uri Request Parameter	OP-request_uri-Unsigned	Support request_uri request parameter with unsigned request	Success	Core	
REQ-WA103-OPENID-SRP 1	scope Request Parameter	OP-scope-All	Scope requesting all claims	Success or Warning	Core	
REQ-WA103-OPENID-SRP 2	scope Request Parameter	OP-scope-address	Scope requesting address claims	Success or Warning	Core	
REQ-WA103-OPENID-SRP 3	scope Request Parameter	OP-scope-email	Scope requesting email claims	Success or Warning	Core	
REQ-WA103-OPENID-SRP 4	scope Request Parameter	OP-scope-phone	Scope requesting phone claims	Success or Warning	Core	
REQ-WA103-OPENID-SRP 5	scope Request Parameter	OP-scope-profile	Scope requesting profile claims	Success or Warning	Core	
REQ-WA103-OPENID-MISCRP1	Misc Request Parameters	OP-Req-NotUnderstood	Request with extra query component	Success or Warning	Core	

REQ-WA103-OPENID-MIS CRP2	Misc Request Parameters	OP-Req-acr_values	Providing acr_values	Success or Warning	Core	
REQ-WA103-OPENID-MIS CRP3	Misc Request Parameters	OP-Req-claims_locales	Providing claims_locales	Success or Warning	Core	
REQ-WA103-OPENID-MIS CRP4	Misc Request Parameters	OP-Req-id_token_hint	Using prompt=none with user hint through id_token_hint	Success or Warning	Core	
REQ-WA103-OPENID-MIS CRP5	Misc Request Parameters	OP-Req-login_hint	Providing login_hint	Success or Warning	Core	
REQ-WA103-OPENID-MIS CRP6	Misc Request Parameters	OP-Req-max_age=1	Requesting ID Token with max_age=1 seconds restriction	Success	Core	
REQ-WA103-OPENID-MIS CRP7	Misc Request Parameters	OP-Req-max_age=10000	Requesting ID Token with max_age=10000 seconds restriction	Success	Core	
REQ-WA103-OPENID-MIS CRP8	Misc Request Parameters	OP-Req-ui_locales	Providing ui_locales	Success or Warning	Core	
REQ-WA103-OPENID-OAB 1	OAuth behaviors	OP-OAuth-2nd	Trying to use authorization code twice should result in an error	Success	Core	
REQ-WA103-OPENID-OAB 2	OAuth behaviors	OP-OAuth-2nd-30s	Trying to use authorization code twice with 30 seconds in between uses must result in an error	Success	Core	
REQ-WA103-OPENID-OAB 3	OAuth behaviors	OP-OAuth-2nd-Revokes	Trying to use authorization code twice should result in revoking previously issued access tokens	Success or Warning	Core	
REQ-WA103-OPENID-CA1	Client Authentication	OP-ClientAuth-Basic-Dynamic	Access token request with client_secret_basic authentication	Success	Core	
REQ-WA103-OPENID-CA2	Client Authentication	OP-ClientAuth-SecretPost-Dynamic	Access token request with client_secret_post authentication	Success or Warning	Core	
REQ-WA103-OPENID-DCR 1	Dynamic Client Registration	OP-Registration-Dynamic	Client registration request	Success or Warning	Unknown	
REQ-WA103-OPENID-DCR 2	Dynamic Client Registration	OP-Registration-Endpoint	Verify that registration_endpoint is published	Success or Warning	Unknown	
REQ-WA103-OPENID-DCR 3	Dynamic Client Registration	OP-Registration-Sector-Bad	Incorrect registration of sector_identifier_uri	Success or Warning	Unknown	
REQ-WA103-OPENID-DCR 4	Dynamic Client Registration	OP-Registration-jwks	Uses keys registered with jwks value	Success or Warning	Unknown	
REQ-WA103-OPENID-DCR 5	Dynamic Client Registration	OP-Registration-jwks_uri	Uses keys registered with jwks_uri value	Success or Warning	Unknown	
REQ-WA103-OPENID-DCR 6	Dynamic Client Registration	OP-Registration-logo_uri	Registration with logo_uri	Success or Warning	Unknown	
REQ-WA103-OPENID-DCR 7	Dynamic Client Registration	OP-Registration-policy_uri	Registration with policy_uri	Success or Warning	Unknown	
REQ-WA103-OPENID-DCR 8	Dynamic Client Registration	OP-Registration-tos_uri	Registration with tos_uri	Success or Warning	Unknown	

REQ-WA103-OPENID-RRP1	request Request Parameter	OP-request-Unsigned	Support request request parameter with unsigned request	Success or Warning	Core	
REQ-WA103-OPENID-RRP1	claims Request Parameter	OP-claims-essential	Claims request with essential name claim	Success or Warning	Core	
REQ-WA103-OPENID-KEY1	Key Rotation	OP-Rotation-OPP-Enc	Can rotate OP encryption keys	Not Required	Not Required	

2.1.2 URLs & Endpoint Support

The RESO OData Transport defines a few standardized URL formatting requirements for ease of use and application interoperability. These requirements are designed to permit standards-compliant applications and servers to interoperate in a pluggable manner requiring minimal configuration. All service URL's must match [OData V4 Part 2 Section 2 URL Components](#) in addition to the additional recommendations detailed in the RESO specification here: [2.3 URL Formatting](#).

The goal is to offer RESO client developers a common structure that is well-understood and highly portable across all server vendors.

NOTE 1-1: These rules were originally approved for RESO Web API 1.0.2. Many of these rules will be replaced by generic OData Testing Rules as noted in the Deprecation Notes column. Deprecated rules will be removed from future standard versions.

Requirement ID	Description	Web API Reference	Compliance Level	Test Results	Deprecation Notes
REQ-WA103-URL1	Support Version in the URL Structures	2.2.1	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-MinC1004
REQ-WA103-URL2	Support Hostname in URL Structures	2.3.1	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-AdvC101101
REQ-WA103-URL3	Support URI Stem in URL Structures	2.3.2	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-AdvC101101 (TBD)
REQ-WA103-END1	Support Service Endpoint	-----	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-MinC1001
REQ-WA103-END2	Support DataSystem Endpoint	2.3.3	N/A	Compliant / Error	RCP - WEBAPI-006 changes this requirement from MUST to MAY . This removes this rule from testing requirements
REQ-WA103-END3	Support Metadata Endpoint	2.3.5	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-MinC1013
REQ-WA103-END4	Support Resource Endpoint	2.3.4	Core	Compliant / Error	

NOTE E4-1: This requirement is satisfied when the testing tool is able to retrieve a record from the "Property" (or another applicant-specified resource). The URL used to retrieve the resource's record **MUST** match one of the example patterns provided in Section 2.3.5.

2.1.3 Query Support

OData offers an extensive query language that enables application developers to create from simple to complex user experiences. The RESO Web API search options are described here: [2.4 Search](#).

NOTE 1-1: These rules were originally approved for RESO Web API 1.0.2. Many of these rules will be replaced by generic OData Testing Rules as noted in the Deprecation Notes column. Deprecated rules will be removed from future standard versions.

Requirement ID	Description	Web API Reference	Compliance Level	Test Results	Deprecation Notes
----------------	-------------	-------------------	------------------	--------------	-------------------

REQ-WA103-Q1	Field names are case sensitive when used in the \$select, \$filter, and \$orderby parameters. Case sensitivity is tested against the values defined in the resource metadata. Case sensitivity MUST be supported.	-----	Core	Compliant / Error	
REQ-WA103-Q2	Servers MAY reject queries that are too complex to accept/handle. Servers MUST generate an appropriate error response and gracefully deny the request.	-----	Core	Compliant / Error	
REQ-WA103-QR1	Search Parameters: Search by UniqueID	2.4.1	Core	Compliant / Error	
REQ-WA103-QR3	Query Support: \$select	2.4.2	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-IntC1003 & REQ-WA103-ODATA-SI-SQOST
REQ-WA103-QR4	Query Support: \$top	2.4.2	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-IntC1005 & REQ-WA103-ODATA-SI-SQOT
REQ-WA103-QR5	Query Support: \$skip	2.4.2	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-IntC1012 & REQ-WA103-ODATA-AdvC1006
REQ-WA103-QO1	Query Support: \$filter	2.4.4	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-IntC1007
REQ-WA103-QO2	Query Support: \$filter - Comparison: eq (equal)	2.4.4	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-IntC100701 & REQ-WA103-ODATA-SI-FE
REQ-WA103-QO3	Query Support: \$filter - Comparison: ne (not equal)	2.4.4	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-FNE
REQ-WA103-QO4	Query Support: \$filter - Comparison: gt (greater than)	2.4.4	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-FGT
REQ-WA103-QO5	Query Support: \$filter - Comparison: ge (greater or equal)	2.4.4	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-FGTOE
REQ-WA103-QO6	Query Support: \$filter - Comparison: lt (less than)	2.4.4	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-FLT
REQ-WA103-QO7	Query Support: \$filter - Comparison: le (less or equal)	2.4.4	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-FLTOE
REQ-WA103-QO8	Query Support: \$filter - Comparison: has	2.4.4	Bronze	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-FH
REQ-WA103-QO9	Query Support: \$filter - Logical: and	2.4.4	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-FAND
REQ-WA103-QO10	Query Support: \$filter - Logical: or	2.4.4	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-FO
REQ-WA103-QO11	Query Support: \$filter - Logical: not	2.4.4	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-FN
REQ-WA103-QO12	Query Support: \$filter - Grouping: ()	2.4.4	Platinum	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-FG

REQ-WA103-QO13	Query Support: \$filter - String: contains	2.4.4	Platinum	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFCT
REQ-WA103-QO14	Query Support: \$filter - String: endswith	2.4.4	Platinum	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFEW
REQ-WA103-QO15	Query Support: \$filter - String: startswith	2.4.4	Platinum	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFWS
REQ-WA103-QO16	Query Support: \$filter - String: tolower	2.4.4	Platinum	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFTL
REQ-WA103-QO17	Query Support: \$filter - String: toupper	2.4.4	Platinum	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFTU
REQ-WA103-QO18	Query Support: \$filter: Date: year	2.4.4	Gold	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFY
REQ-WA103-QO19	Query Support: \$filter: Date: month	2.4.4	Gold	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFMON
REQ-WA103-QO20	Query Support: \$filter: Date: day	2.4.4	Gold	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFDAY
REQ-WA103-QO21	Query Support: \$filter: Date: hour	2.4.4	Gold	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFH
REQ-WA103-QO22	Query Support: \$filter: Date: minute	2.4.4	Gold	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFMIN
REQ-WA103-QO23	Query Support: \$filter: Date: second	2.4.4	Gold	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFSEC
REQ-WA103-QO24	Query Support: \$filter: Date: fractionalseconds	2.4.4	Gold	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFFS
REQ-WA103-QO25	Query Support: \$filter: Date: Date	2.4.4	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFD
REQ-WA103-QO26	Query Support: \$filter: Date: Time	2.4.4	n/a	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFT Requirement removed by RCP - WEBAPI-007
REQ-WA103-QO27	Query Support: \$filter: Date: Now	2.4.4	Core	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFNOW
REQ-WA103-QO28	Query Support: \$orderby	2.4.4	Bronze	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOOB & REQ-WA103-ODATA-IntC1017 & REQ-WA103-ODATA-AdvC1008 & REQ-WA103-ODATA-AdvC100904
REQ-WA103-QO29	Query Support: \$expand	2.4.4	Platinum	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOE & REQ-WA103-ODATA-MinC1012

REQ-WA103-QM1	Support Only Correct Data Types: Edm.Boolean, Edm.Byte, Edm.Date, Edm.DateTimeOffset, Edm.Decimal, Edm.Double, Edm.Int16, Edm.Int32, Edm.Int64, Edm.SByte, Edm.String, Edm.TimeOfDay, Edm.Geography, Edm.GeographyPoint, Edm.GeographyLineString, Edm.GeographyPolygon, Edm.GeographyMultiPoint, Edm.GeographyMultiLineString, Edm.GeographyMultiPolygon, Edm.EnumType.	2.4.3	Platinum	Compliant / Error	RESO allows for a sub-set of the " 4.4 Primitive Types " defined in the OData Standard as defined in 2.4.3 Data Types .
REQ-WA103-QM2	Support Lambda Operators	2.4.5	Platinum	Compliant / Error	Removed per Transport Work Group Vote (2017-03-07). Replaced by REQ-WA103-ODATA-SI-FANY & REQ-WA103-ODATA-SI-FALL
REQ-WA103-QM3	Support Literals: \$any	2.4.6	Platinum	Compliant / Error	Formerly \$it - Changed by Transport Work Group Vote (2017-03-07). Replaced by REQ-WA103-ODATA-SI-FANY
REQ-WA103-QM4	Support Literals: \$all	2.4.6	Platinum	Compliant / Error	Formerly \$root - Chanaged by Transport Work Group Vote (2017-03-07). Replaced by REQ-WA103-ODATA-SI-FALL
REQ-WA103-QM5	Support Geospatial Search Implementation	2.4.7	Platinum	Compliant / Error	Replaced by REQ-WA103-ODATA-SI-SQOFGD & REQ-WA103-ODATA-SI-SQOFGI & REQ-WA103-ODATA-SI-SQOFG L
REQ-WA103-QM6	Support Annotations	2.4.8	Bronze	Compliant / Error	
REQ-WA103-QM7	Support Single Value Lookups	2.4.9	Bronze	Compliant / Error	
REQ-WA103-QM8	Support Multi Value Lookups	2.4.10	Bronze	Compliant / Error	

2.1.4 RESO Data Dictionary Support

There is no requirement for the RESO Data Dictionary to be implemented within the RESO Web API Standard for applicants to receive RETS Web API Certification.

The RESO Data Dictionary may be represented using the RESO Web API Standard. However, the Data Dictionary Certification is awarded separately.

2.1.5 Response Code Support

Server vendors **MUST** use standard HTTP response codes to communicate successful transactions and all server errors. This conforms with OData and is accepted as a generally desired practice across all RESO transport standards.

NOTE 0-1: These testing rules are in reference to [2.5.2 HTTP Response Codes](#) found in the specification.

REQ-WA103-RC1: A compatible server implementation **MUST** return a valid HTTP status **code** for each request indicating the status of the request when ATOM-XML is requested.

NOTE 1-1: When a JSON response is requested, a server **SHOULD** return a valid HTTP status code as required for ATOM-XML responses.

REQ-WA103-RC2: If the response was not successful, the server **MAY** include an error **message** in the body of the HTTP response. There is a defined response body for JSON but there is no explicit requirement in the OData standard.

The following table includes additional requirements about the specific response codes.

Requirement ID	Description	Web API Reference	Compliance Level	Test Results
REQ-WA103-RC3	Support Response Code: 200 (OK)	2.5.2	Core	Compliant / Error
REQ-WA103-RC4	Support Response Code: 202 (Accepted)	2.5.2	n/a	Not Required for "read-only" servers
REQ-WA103-RC5	Support Response Code: 400 (Bad Request)	2.5.2	Core	Compliant / Error
REQ-WA103-RC6	Support Response Code: 403 (Forbidden)	2.5.2	Core	Compliant / Error (See NOTE 6-1)
REQ-WA103-RC7	Support Response Code: 404 (Not Found)	2.5.2	Core	Compliant / Error
REQ-WA103-RC8	Support Response Code: 413 (Retry Entity Too Large)	2.5.2	n/a	Not Tested but SHOULD be implemented
REQ-WA103-RC9	Support Response Code: 415 (Unsupported Media)	2.5.2	Core	Duplicate of REQ-WA103-ODATA-MinC100501 . This rule preserved so all HTTP tests are documented in the same section of the testing rules.
REQ-WA103-RC10	Support Response Code: 429 (Too Many Requests)	2.5.2	n/a	Not Tested but SHOULD be implemented
REQ-WA103-RC11	Support Response Code: 500 (Internal Server Error)	2.5.2	n/a	Not Tested but SHOULD be implemented
REQ-WA103-RC12	Support Response Code: 501 (Not Implemented)	2.5.2	Core	Compliant / Error

NOTE 6-1: A server **MAY** return HTTP 404 (Not Found) instead of HTTP 403 (Forbidden) at the developer's discretion. Applicants **MUST** inform RESO Compliance Testers if HTTP 403 is not implemented to remove this from testing procedures.

2.1.6 Property Facet Support

OData Property Facets allow a model to provide additional constraints or data about the value of structural properties. Facets are expressed as attributes on the property element. Facets apply to the type referenced in the element where the facet attribute is declared. If the type is a collection, the facets apply to the type of elements in the collection. The RESO Web API requires implementation of specific [OData V4 Part 3 Section 6.2 Property Facets](#).

Requirement ID	Description	OData Reference	Compliance Level	Test Results	RESO Compliance Notes
REQ-WA103-L1	Required Property Facet Support: Attribute MaxLength	6.2.2	Core	Compliant / Error	This rule applied for the following data types: Edm.String
REQ-WA103-P1	Required Property Facet Support: Attribute Precision	6.2.3	Core	Compliant / Error	This rule applied for the following data types: Edm.Decimal, Edm.DateTimeOffset
REQ-WA103-P2	Attribute Precision Length MUST be a positive integer and MUST be a non-negative integer between 0 and 12 for a temporal property	6.2.3	Core	Compliant / Error	Added per RCP - WEBAPI-001
REQ-WA103-S1	Required Property Facet Support: Attribute Scale	6.2.4	Core	Compliant / Error	This rule applied for the following data types: Edm.Decimal
REQ-WA103-S2	Attribute Scale Length MAY be a non-negative integer or "variable"	6.2.4	Core	Compliant / Error	Added per RCP - WEBAPI-001

NOTE 1: Any data type **NOT** explicitly listed with the rules above **MAY** be provided **WITHOUT** any property facets.

NOTE 2: Additional property facets **MAY** be provided **IN ADDITION** to those **REQUIRED** by the rules above as long as it does not break OData standards found in [6.2 Property Facets](#).

NOTE 3: It is possible to have a compliant data structure without using the precision or scale attributes if Edm.Double is used instead of Edm.Decimal. (OData [6.2 Property Facets](#) does not state that precision or scale attributes are allowed for Edm.Double.)

NOTE 4: Attribute Scale "variable" value is NOT COMPLIANT with RESO Data Dictionary Testing Rule [REQ-DD160WA1X-S-1 Note 1-1](#).

3.0 RESO Web API Certification Rules

This section contains all of the rules that RESO will use in awarding RESO Web API Certificates. The specific set of rules that must be passed for "Compliance" are discussed in Section 2.

Certification is awarded when all requirements detailed in this testing rules document has been satisfied for any given certification level.

3.1 Compliance Levels Definition Summary

3.2 RESO Web API Server Certification Level Testing Rules

3.1 Compliance Levels Definition Summary

The RESO Web API Certification has many different levels. This is an effort to provide additional recognition to those who implement more than the minimum requirements. These level descriptions are for both Server and Client Certificates.¹ Each server and client compliance level has specific requirements detailed in sections later in this document.

Level Name	Objective	Target Year ²	Description Summary
Core	Minimum	2016-2017	All Core Level functionality is implemented. This is the minimum functionality for a RESO Web API Server to function. Compliance Warnings and Notices MAY be allowed.
Bronze	Parity	2018	All Bronze Level functionality is implemented. This includes functionality similar to RETS 1.x Servers. Compliance Warnings and Notices MAY be allowed.
Silver	Advanced	2019	All Silver Level functionality is implemented. This includes advanced business cases previously not addressed by the RETS 1.x Specification. Compliance Warnings and Notices MAY be allowed.
Gold	Complete	2020	All RESO Web API functionality is implemented. Compliance Notices MAY be allowed. Compliance Warnings are NOT allowed. Compliance Notices MAY be allows
Platinum	Maximum	2021	All RESO Web API functionality is implemented. Compliance Warnings and Notices NOT allowed.

Every functionality within the RESO Web API specification has been assigned to one of these different levels. All functionality at that level **MUST** be implemented **AND** compliant to be certified at that level. Additionally, all aspects of a lower compliance level **MUST** be satisfied before receiving a higher compliance level. For example, "Core" is a requirement for "Bronze", "Bronze" for "Silver", "Silver" for "Gold", and "Gold" for "Platinum." Generally speaking, failing at a level will result in receiving certification at the next level below.

Note 1: "Functionality Implemented" may differ for between Servers and Clients. Generally, a functionality is implemented on a server if it can provide that feature or implemented on a client if it can request or accept that feature from the server. More specific details may be found in [Section 2 - Compliance Rules](#) of this document.

Note 2: The Compliance Level Target Year is the year where this Compliance Level will become required. For example, beginning January 1, 2018, the Bronze (Parity) level of compliance is REQUIRED for certification. Beginning January 1, 2021, the Platinum (Perfection) compliance level is REQUIRED for certification.

3.2 RESO Web API Server Certification Level Testing Rules

3.2.1 RESO Web API Server Core Certification (Minimum)

3.2.2 RESO Web API Server Bronze Certification (Parity)

3.2.3 RESO Web API Server Silver Certification (Advanced)

3.2.4 RESO Web API Server Gold Certification (Complete)

3.2.5 RESO Web API Server Platinum Certification (Maximum)

3.2.1 RESO Web API Server Core Certification (Minimum)

RESO Web API Server Core Certification (Minimum) is the first of the compliance levels. Any description of a RESO Web API Certification without distinction will refer to this minimum level.

These are the minimum requirements that **MUST** be satisfied to receive certification. Any non-compliant core functionality will prevent receiving this certification.

REQ-WS100-WSC-1: Satisfies all requirements for RESO Web API Server Core certification.

NOTE: The "Core Compliance" requirements will roll up into the Bronze requirements at the end of 2017.

3.2.2 RESO Web API Server Bronze Certification (Parity)

RESO Web API Server Bronze Certification (Parity) is the first of the certification levels beyond the minimum "Core" certification. Any non-compliant Bronze (Parity) functionality will prevent receiving this certification.

NOTE 1: The term "Parity" implies those obtaining this certification means that the RESO Web API Server is able to perform the same functionality as a RETS 1.x Server. (Exact parity functionality MAY vary as determined by the RESO Transport Workgroup.)

REQ-WS100-WSB-1: All RESO Web API Server Bronze (Parity) functionality **MUST** be found compliant. Bronze (Parity) functionality found within the applicant's server implementation that is **NOT** found to be compliant will not be awarded Bronze certification but may be eligible for lower levels.

REQ-WS100-WSB-2: Satisfies **ALL** requirements for RESO Web API Server Core (Minimum) certification.

NOTE: The "Bronze Compliance" requirements will roll up into the Silver requirements at the end of 2018.

3.2.3 RESO Web API Server Silver Certification (Advanced)

RESO Web API Server Silver Certification (Advanced) is the first level where the presence of cautionary warnings impacts certification results. Any non-compliant Silver (Advanced) functionality will prevent receiving certification.

NOTE: The term "Advanced" implies obtaining this certification means that the RESO Web API Server is able to perform the more functionality than a RETS 1.x Server. This MAY include functionality exclusively available to the RESO Web API. (Exact advanced functionality MAY vary as determined by the RESO Transport Workgroup.)

REQ-WS100-WSS-1: All RESO Web API Server Silver (Advanced) functionality **MUST** be found compliant. Silver (Advanced) functionality found within the applicant's server implementation that is **NOT** found to be compliant will not be awarded Silver certification but may be eligible for lower levels.

REQ-WS100-WSS-2: Satisfied all requirements for RESO Web API Server Bronze (Parity) certification.

NOTE: The "Silver Compliance" requirements will roll up into the Gold requirements at the end of 2019.

3.2.4 RESO Web API Server Gold Certification (Complete)

RESO Web API Server Gold Certification (Complete) is the certification level where **ALL** of the RESO Web API functionality has been implemented. Any non-compliant Gold (Complete) functionality will prevent receiving this certification.

REQ-WS100-WSG-1: All RESO Web API Server Gold (Complete) functionality **MUST** be found compliant. Gold (Complete) functionality found within the applicant's server implementation that is **NOT** found to be compliant will not be awarded Gold certification but may be eligible for lower levels.

REQ-WS100-WSG-2: No Compliance Warnings of any type are allowed. Compliance Notices are allowed, if applicable.

REQ-WS100-WSG-3: Satisfied **ALL** requirements for RESO Web API Silver (Advanced) certification.

NOTE: The "Gold Compliance" requirements will roll up into the Platinum requirements at the end of 2020. The Platinum Certification will become the only level for Data Dictionary certification in 2021.

3.2.5 RESO Web API Server Platinum Certification (Maximum)

RESO Web API Server Platinum Certification (Maximum) is the certification level where **ALL** of the RESO Web API functionality has been implemented without warning or notice. Any non-compliant Platinum (Maximum) functionality will prevent receiving this certification. Platinum is the highest level of certification. This is the 100% compliance level.

REQ-WS100-WSP-1: All RESO Web API Server Platinum (Maximum) functionality **MUST** be found compliant. Platinum (Maximum) functionality found within the applicant's server implementation that is **NOT** found to be compliant will not be awarded Platinum certification but may be eligible for lower levels.

REQ-WS100-WSP-2: No Cautionary Warnings or Notices of any type are allowed.

REQ-WS100-WSP-3: Satisfies **ALL** requirements for RETS Web API Gold (Complete) certification.

| **NOTE:** The Platinum Compliance will become the only level for RESO Web API Certification in 2021.

4.0 RESO Web API Report Card and Specifications

The RESO Web API Report Card is used to report to the applicant the certification findings. This will include a list of the testing results from testing.

The exact format will be determined by the RESO Compliance Staff with input from the RESO Transport Workgroup.

Change Log

Web API Testing Rules Change Log

Version 1.0.3

[2.1.1 Non-RESO Technology Standards included in RESO Web API Compliance Testing Rules](#)

- Expanding text to explain changes in sub-sections

[2.1.1.1 OData 4.0 OASIS Standard](#)

- Single generic rule "REQ-WA100-OASIS1" with individual rules specifically required by RESO Standard.
- Includes new pages for "Conformance" and "Service Implementation" Rules.

[2.1.1.1.1 OData 4.0 OASIS Standard: Conformance Rules](#)

- New Page

[2.1.1.1.2 OData 4.0 OASIS Standard: Service Implementation Rules](#)

- New Page

[2.1.1.2 OpenID Connect Standard](#)

- Single generic rule "REQ-WA100-OPENID1" replaced with individual rules specifically required by RESO Standard for each of the acceptable security implementations.
- Adding testing rules for OAuth 2 Client Credentials Security: **REQ-WA103-SC3** and **REQ-WA103-CC1**.

[2.1.2 URLs & Endpoint Support](#)

- Added "Deprecation Notes" Column to provide information on the Non-RESO OData Requirement Replacement Testing Rules.
- **RCP - WEBAPI-006** changes the **REQWA103-END2** requirement from **MUST** to **MAY**. This removes this rule from testing requirements.
- Added **NOTE E4-1** to provide clarity to how **REQ-WA103-END4** is tested.

[2.1.3 Query Support](#)

- Added "Deprecation Notes" Column to provide information on the Non-RESO OData Requirement Replacement Testing Rules
- Transport Work Group (2017-03-06) voted (1) to remove \$it and \$root from testing rules and (2) to add \$any and \$all. **REQ-WA100-QM3** and **REQ-WA100-QM4** changed to reflect this change (re-using rule IDs as they are already deprecated by **REQ-WA103-ODATA-SI-FA NY** & **REQ-WA103-ODATA-SI-FALL**.)
- Added the allowed OData Primitive Types that are allowed for rule **REQ-WA103-QM1**.
- Changed **REQ-WA103-QO26** to N/A to reflect **RCP - WEBAPI-007 Section 2.4.4: Remove required filter function time()**. Change also made for [2.1.1.1.2](#).

[2.1.5 Response Code Support](#)

- Added link to the standard's page: [2.5.2 HTTP Response Codes](#)
- **REQ-WA103-RC1**: Added Note 1-1 that recommends JSON-formatted responses also include valid HTTP Response codes.
- **REQ-WA103-RC4 (HTTP 202)**: The "Accepted" response code is removed as a requirement as it deals with UPDATE functionality not included in the RESO Web API 1.0.3 Standard.
- **REQ-WA103-RC8 (HTTP 413)**: The "Retry Entity Too Large" response code is removed as a tested requirement as the testing tool platform cannot produce a request to trigger this code.
- **REQ-WA103-RC9 (HTTP 415)**: The "Unsupported Media Type" response code is replaced by **REQ-WA103-ODATA-MinC100501**.
- **REQ-WA103-RC10 (HTTP 429)**: The "Too Many Requests" response code is removed as a tested requirement as the testing tool platform cannot produce a request to trigger this code.
- **REQ-WA103-RC11 (HTTP 500)**: The "Internal Server Error" response code is removed as a tested requirement as the testing tool platform cannot produce a request to trigger this code.
- The ID **"REQ-WA103-RC9"** was used twice. Following codes (10-12) were renumbered.

[2.1.6 Property Facet Support](#)

- Added "RESO Compliance Notes" Column to the requirements table
- Added notes to the rules to provide clarity on which data types must comply with which rules. (See table and new notes for details.)
- Added new requirements and notes from **RCP - WEBAPI-001**: **REQ-WA103-P2**, **REQ-WA103-S2**, and **NOTE 4**.

Version 1.0.2.1

[2.1.3 Query Support](#)

- Transport Workgroup Meeting (2016-09-12):

- APPROVED: Motion carries to remove the verbiage “required” and “optional” for REQ-QA100-QR1 through REQ-WA100Q029.
- APPROVED: Motion carries to remove REQ-QA100-QR2 altogether from the RESO Web API Server Testing Rules.

Version 0.0 (Draft)

This documentation is based on an existing [Data Dictionary Certification Testing Rules](#). Due to large number of changes required to convert this for the Web API Standard, specific changes will not be recorded until after this document has been reviewed by the [RESO Transport Workgroup](#).