Requirements and Recommendations for OVAL Adoption and Use

Date: August 22, 2013 **Document version:** 1.1

Table of Contents

Introduction

This document outlines the requirements and recommendations that need to be satisfied in order for a product, service, Web site, database, or advisory/alert to properly implement support for OVAL. At the same time, these requirements describe the supported and recommended ways of making use of OVAL Content and other capabilities that leverage OVAL.

Please send any comments or concerns about this document to oval@mitre.org.

Definitions

The following terms are used throughout this document:

Assessment Method – A specific method that a product or service uses to evaluate an OVAL Definition. OVAL supports assessment through:

1. Query to a database of an endpoint's (i.e., any computing device that can be connected to a network such as a system, network appliance, mobile device, etc.) current configuration settings.
2. An assessment of state by a host-based sensor.
3. An assessment of state by a remote-scanning sensor.

Capability – A specific function or functions of a product, service, or repository.

Endpoint – As stated in the Internet Engineering Task Force's (IETF) "Network Endpoint Assessment (NEA): Overview and Requirements, RFC 5209" document, an endpoint is any computing device that can be connected to a network such as a computer system, server, network appliance, mobile device, etc. "Such devices normally are associated with a particular link layer address before joining the network and potentially an IP address once on the network."

Owner – The creator, seller, or maintainer of a product, service, or repository.

User – A consumer (or potential consumer) of a product, service, or repository.

Product – A security application, appliance, or security database that has one or more capabilities.

Repository – An implicit or explicit collection of security elements that support a product (e.g., a vulnerability database, a set of signatures in an assessment product or service, or a web site).

Correctness Testing – The process of determining whether a product, service, or repository has correctly adopted OVAL.

Test Results – Data representing the outcome of correctness testing.

Review Authority – An entity that performs correctness testing and is authorized to formally acknowledge that a product, service or repository has correctly adopted OVAL (The MITRE Corporation is the only review authority at this time).

Adoption Capabilities

The OVAL Adoption Program is based on five different capabilities, each targeting a different usage of the OVAL Language. These capabilities enable members of the OVAL community to easily understand how a given product is using the OVAL Language and how it might suit their needs.

Authoring Tool	A product that aids in the process of creating new OVAL files (including products that consolidate existing OVAL Definitions into a single file).
Definition Evaluator	A product that uses an OVAL Definition to guide evaluation and produces OVAL Results (full results) as output using one or more of the OVAL supported assessment methods.
Definition Repository	A repository of OVAL Definitions made available to the community (free or pay).
Results Consumer	A product that accepts OVAL Results as input and either displays those results to the user, or uses the results to perform some action (remediation, SIM, etc.).
System Characteristics Producer	A product that generates a valid OVAL System Characteristics document based on the details of an endpoint using one or more of the OVAL-supported assessment methods.

Common Adoption Requirements

The following requirements apply to all capabilities that are implementing support for OVAL, regardless of the capability that they plan to implement. If the product, service, or repository satisfies all applicable requirements, then the owner shall receive formal acknowledgement of correctly adopting OVAL. However, the owner shall not advertise the formal acknowledgement for adopting OVAL until the review authority has granted such.

General

These requirements deal with general aspects of OVAL Adoption.

1.1 – The owner shall be a valid legal entity (i.e., an organization or a specific individual, with a valid phone number, email address, and street address).

1.2 – The owner shall agree to abide by all of the mandatory OVAL Adoption Requirements, which includes the mandatory requirements for the specific capability.

1.3 – The owner shall provide the review authority with a technical point of contact that is qualified to answer questions regarding any OVAL-related functionality of the product, service, or repository and coordinate the preparation of the product, service, or repository for correctness testing.

1.4 – The owner shall provide the review authority with a completed "OVAL Adoption Questionnaire Form." This form will be sent once the declaration process has been satisfied. Please see the section "How to Declare Your Product, Service, or Repository as an OVAL Adopter" for more information.

1.5 – The owner shall provide the review authority with free access to items needed to perform correctness testing, including the test results and/or the repository, in order to determine compliance with all associated requirements.

1.6 – The owner shall work with the review authority to make the product, service, or repository available for correctness testing.

1.7 – As a part of receiving formal acknowledgement of correctly adopting OVAL, the owner shall agree to support the review authority in follow-on testing activities, where appropriate types of files will be exchanged with other organizations attempting to prove the correctness of their product, service, or repository. This will be managed by the review authority and kept to reasonable levels of effort for all involved.

1.8 – The product shall provide additional value or information beyond that which is provided in OVAL itself. Therefore, forwarding or providing references to a single source of OVAL Definitions that have been created by someone else is not by itself considered to be sufficient for formal acknowledgement of correctly adopting OVAL.

1.9 – The product, service, or repository shall be available to the public or a set of consumers.

1.10 – The product, service, or repository shall clearly state the schema(s) and version with which it is compatible.

Correctness

2.1 – The owner shall have in place a means for the user to submit correctness errors found in the use of OVAL and in any OVAL content being produced by the product, service, or repository.

2.2 – The owner shall have a plan in place to address any correctness errors reported to it.

2.3 – The owner shall address any correctness errors reported to it within a reasonable time frame after the error was initially reported.

Documentation

The following requirements apply to documentation that is provided with an OVAL adopter's product, service, or repository.

3.1 – The product shall include in its documentation a brief description of OVAL and OVAL Adoption, which can include verbatim portions of documents from the OVAL Web site.

3.2 – The product shall clearly state in its documentation any component schemas or individual tests that it does not support. For example, if a product is applying for formal acknowledgement of correctly adopting OVAL as a Definition Evaluator and does not support the Windows metabase test, then the product, service, or repository documentation shall state this incompatibility.

3.3 – The *product* or *service* shall clearly state in its documentation which of the three OVAL-supported assessment method(s) the product or service utilizes.

3.4 – The product, service, or repository shall clearly state in its documentation the procedure that a user must follow to submit correctness errors found in any OVAL content being produced by the product.

3.5 – If the documentation included with the product, service, or repository includes an index, then it shall include references to OVAL-related documentation under the term "OVAL."

Validity

OVAL Adopters are required to work with valid documents. This helps to ensure that information is being formatted correctly and that the structure of the document follows the OVAL Language.

4.1 – The product, service, or repository shall validate all OVAL content (both produced and consumed) using W3C XML Schema validation against the version of the OVAL Language with which it is stated to comply.

4.2 – The product, service, or repository shall report any W3C XML Schema validation errors to the user.

4.3 – The product, service, or repository shall validate all OVAL content (both produced and consumed) using Schematron validation against the version of the OVAL Language with which it is stated to comply.

4.4 – The product, service, or repository shall report any Schematron validation errors to the user.

Specific Capability Requirements

The following requirements are related to the specific adoption capabilities previously outlined and only apply to products, services, or repositories that are looking to gain formal acknowledgement of correctly adopting OVAL for that specific capability.

System Characteristics Producer

These requirements apply to all products or services that intend to generate information about a specific endpoint in the OVAL System Characteristics Schema format.

5.1 – The product or service shall use a unique item ID (unique on a per file basis) for each specific system characteristic item it collects.

5.2 – The product or service shall generate system characteristics items that contain the exact system configuration values gathered at the time the product or service is executed against the endpoint.

5.3 – The product or service that uses an OVAL Definition document to generate system characteristics items shall include a collected_objects section with a system characteristics object for each object collected in the input OVAL Definition document.

Definition Repository

These requirements apply to all repositories that intend to provide a collection of information in the OVAL Definition Schema format.

6.1 – All OVAL Definitions, Tests, Objects, States, and Variables shall contain a unique ID with respect to all other OVAL Definitions, Tests, Objects, States, and Variables in the OVAL community.

6.2 – Each repository should use its own unique constant namespace portion of the ID across all OVAL content.

6.3 – Each OVAL Definition, Test, Object, State, and Variable shall keep the same ID across its existence. This enables users to reference these items based on the stable ID. An existing item should not be rewritten for some other purpose as users may be referencing the item in their own content.

6.4 – Each update or modification of an OVAL Definition, Test, Object, State, or Variable in the repository shall result in the item’s version being incremented. Similarly, each item that references the updated or modified item shall also have its version incremented. This cascading of version updates up to referencing items does not need to extend beyond referencing OVAL Definitions since OVAL Definitions provide a logical unit.

6.5 – The OVAL Definition metadata shall be consistent with the OVAL Definition content (e.g., the affected family shouldn't be 'windows' if the tests are examining Red Hat RPM's). Additionally, the metadata shall reflect all of the OVAL Definition’s content, which means the metadata may need to have sections for each affected family when an OVAL Definition applies to more than one family.

6.6 – A repository that contains an OVAL Definition to cover a specific vulnerability shall include, when available, a CVE name as a reference.

6.7 – A repository that contains an OVAL Definition to check for a specific configuration state shall include, when available, a CCE ID as a reference.

6.8 – A repository that contains an OVAL Definition to check for a specific platform shall include, when available, a CPE name as a reference.

6.9 – The owner shall document the process by which a user can retrieve content updates.

Authoring Tool

These requirements apply to all products or services that are designed to help facilitate the creation or modification of OVAL content.

7.1– An authoring tool shall provide a search interface to allow the user to search for OVAL Definitions, Tests, Objects, States, and Variables by ID.

7.2– An authoring tool should encourage the reuse of existing OVAL Definitions, Tests, Objects, States, and Variables.

7.3– An authoring tool should allow the user to invoke validation on a document that is written for the OVAL Language and report all W3C XML Schema and Schematron errors to the user.

7.4– An authoring tool shall allow the user to import and edit existing OVAL content.

7.5– An authoring tool shall allow the user to export the content, created by the tool, as valid OVAL Language documents.

7.6– An authoring tool should report duplicate content to the user.

7.7– An authoring tool shall provide value and capability above and beyond the capability of a XML editor.

Definition Evaluator

These requirements apply to all products or services that intend to evaluate a specified endpoint using, as input, information provided in the OVAL Definition Schema format. Once evaluation has been performed, the results must be available in the OVAL Results Schema format.

8.1 – The user shall be able to determine which OVAL Definitions are being evaluated.

8.2 – The user shall be able to examine the details of each OVAL Definition being evaluated. This requirement ensures that the OVAL Definitions are open to the user allowing them to see how a specific issue is being tested.

8.3 – If the product or service does not consume OVAL Definitions at runtime, the owner shall document the process by which a user can submit OVAL Definitions to the owner for interpretation by the product. This includes stating how quickly definitions submitted to the owner are made available to the product.

8.4 – The product or service shall be capable of interpreting all of the logic within each OVAL Definition and subsequent OVAL Tests in accordance with the stated logical operators.

8.5 – The product or service shall determine the result of evaluating the target endpoint based on the details specified in the OVAL Definition.

8.6 – The user shall be able to determine the result of all OVAL Definitions used in the evaluation of the target endpoint.

8.7 – The product or service shall generate accurate, predictable, and repeatable results when using a specific set of OVAL Definitions and endpoint state information.

8.8 – The results generated by the product or service shall be available in the full OVAL Results format. This allows other products or services that want to leverage detailed evaluation information, to obtain the information as desired. Thin results may be available as well, but full results are required.

8.9 – When an OVAL Definition has been evaluated more than once on a single endpoint, each time with different values for the variables, the OVAL Results file shall include unique variable instance values for each individual case.

8.10 – A product or service shall use a result of "not evaluated" for all OVAL Definitions that are part of the original OVAL Definition file, but are not being reported on. This satisfies requirement 8.6 for the given OVAL Definition.

8.11 – Any use or translation of an OVAL Definition into the internal language of the product or service shall reflect the same logic as the original OVAL Definition.

Results Consumer

These requirements apply to all products or services that intend to consume information in the OVAL Results Schema format.

9.1 – For each endpoint defined in the OVAL Result file being consumed, the user shall be able to determine the specific OVAL Definitions that are being reported on.

9.2 – The user shall be able to examine the details of the OVAL Results file being consumed. This can be as simple as allowing the user to open the XML file. The point of this requirement is to make sure that the OVAL Results used are open to the user allowing them to examine the data being reported.

9.3 – If the product or service does not consume OVAL Results files at runtime, the owner shall document the process by which a user can submit OVAL Results files to the owner for interpretation by the product or service. This includes stating how quickly files submitted to the owner are made available to the product or service.

Review Authority Requirements

The following are requirements pertaining to OVAL Adoption that the review authority must adhere to.

10.1 – The review authority shall clearly identify the version of the adoption, the version of the requirements document, and the version of the OVAL Language that was used to determine formal adherence to the OVAL Adoption Requirements for each product, service, or repository.

10.2 – The review authority shall define and publish sample test materials.

10.3 – The review authority shall publicize information on how to participate in correctness testing so that organizations can prepare as much in advance as possible.

10.4 – The review authority shall provide a point of contact for arranging correctness testing for capabilities declaring support for OVAL that have completed the "OVAL Adoption Questionnaire Form."

10.5 – The review authority may re-test a product, service, or repository that has been formally acknowledged for Adopting OVAL at the discretion of the review authority.

Revocation

If the review authority has verified that a product, service, or repository has correctly adopted OVAL, but at a later time the review authority has evidence that the requirements are no longer being met, then the review authority may revoke its approval and the product, service, or repository will no longer be formally acknowledged as correctly adopting OVAL. The following are the requirements that the review authority must follow in order to revoke the acknowledgement.

11.1 – The review authority shall provide the product, service, or repository owner with a warning of revocation at least two (2) months before revocation is scheduled to occur.

11.2 – The review authority may delay the date of revocation.

11.3 – If the review authority has found that the actions or claims of the owner are intentionally misleading, then the review authority may skip the warning period. The review authority may interpret the phrase "intentionally misleading" as it wishes.

11.4 – If the review authority finds that the actions of the owner with respect to the adoption requirements are intentionally misleading then revocation shall last a minimum of one year.

11.4 – The review authority shall identify the specific requirements that are not being met.

11.5 – If the owner believes that the requirements are being met, then the owner shall respond to the warning of revocation by providing specific details that indicate why the product, service, or repository meets the requirements under question.

11.6 – If the owner modifies the product, service, or repository so that it complies with the requirements in question, during the warning period, then the review authority should end the revocation action for the product, service, or repository.

11.7 – The review authority shall publicize that the formal acknowledgement of the correct adoption of OVAL has been revoked for the product, service, or repository.

11.8 – The review authority may publicize the reason for revocation.

How to Declare Your Product, Service, or Repository as an OVAL Adopter

To begin the OVAL Adoption process, send an email to oval@mitre.org requesting the "OVAL Adoption Declaration Form." This form, along with a copy of the "Requirements and Recommendations for OVAL

Adoption and Use," will be sent to you for review. Once the form has been completed, email it back to oval@mitre.org for processing.

Additional Information

For additional information, please see the OVAL Adoption Process and OVAL Technical Use Cases pages on the OVAL Web site (https://oval.mitre.org/), or contact us at oval@mitre.org.