TCG Trusted Network Connect

SCAP Messages for IF-M

Specification Version 1.0
Revision 16
3 October 2012
Public Review

Contact:

Please submit comments by January 15, 2012 to scap-messages-comments@trustedcomputinggroup.org

Review all comments received at:
https://www.trustedcomputinggroup.org/resources/comments_for_tnc_scap_messages_for_ifm

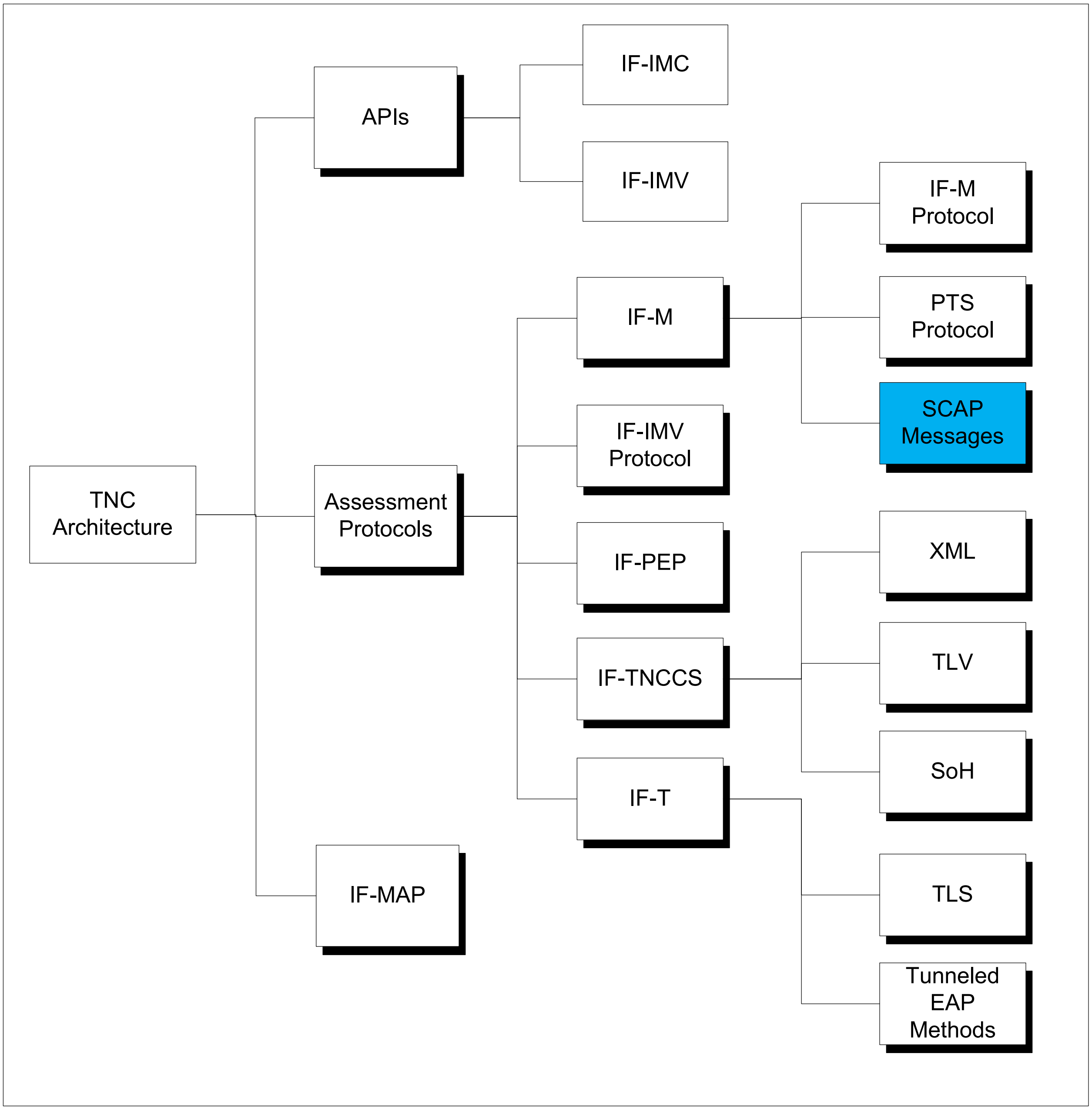
Work in Progress
This document is an intermediate draft for comment only and is subject to change without notice. Readers should not design products based on this document.

TCG PUBLIC REVIEW

Disclaimer

THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

IWG TNC Document Roadmap



Acknowledgement

The TCG wishes to thank all those who contributed to this specification. This document builds on considerable work done in the various working groups in the TCG.

Special thanks to the members of the TNC contributing to this document:

Authors of the PTS Protocol Binding to TNC IF-M, from which some sections of this document were lifted.	
Dave Waltermire (NIST)	
Lisa Lorenzin (Juniper)	
Clifford Kahn (Juniper)	
Steve Venema (Boeing)	
James Tan (Infoblox)	
David Vigier (Infoblox)	
Ira McDonald (High North Inc.)	
Kent Landfield (Intel)	
Stephen Hanna (Juniper)	
Paul Sangster (Symantec)	
Charles Schmidt (MITRE)	

Table of Contents

1 Introduction

1.1 Scope and Audience

The Trusted Network Connect Working Group (TNC) is defining an open solution architecture that enables network operators to enforce policies regarding endpoint integrity when granting access to a network infrastructure. The Security Content Automation Protocol (SCAP) [3], created by the United States National Institute of Standards and Technology (NIST), describes the coordinated use of a suite of standards that support description, automated assessment, and results storage of enterprise security information. SCAP can be used to support vulnerability management, configuration assessment, inventory tracking, and patch management using standards that have broad vendor support. The IF-M for SCAP interface is used to communicate SCAP information between IMVs and IMCs using the IF-M interface, as shown in Figure 1 below.

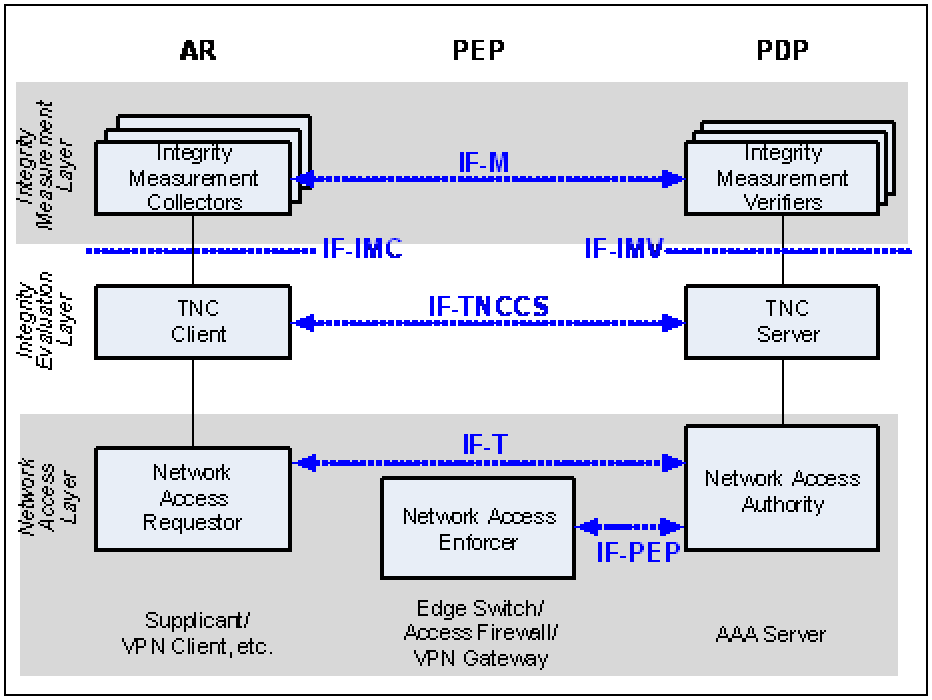

AR
PEP
PDP
Integrity Measurement Layer
Integrity Measurement Collectors
IF-M
Integrity Measurement Verifiers
IF-IMC
IF-IMV
Integrity Evaluation Layer
TNC Client
IF-TNCCS
TNC Server
Network Access Layer
Network Access Requestor
IF-T
Network Access Authority
Network Access Enforcer
IF-PEP
Supplicant/ VPN Client, etc.
Edge Switch/ Access Firewall/ VPN Gateway
AAA Server

Figure 1 - TNC Architecture

This specification defines the SCAP messages carried over IF-M that are used to communicate instructions for SCAP assessments and the corresponding results between the server's IMVs and the client's IMCs.

Before reading this specification any further, the reader should review and understand the TNC architecture as described in [1]. If the reader is building a TNC Client that supports IF-IMC, the reader is encouraged to read [5] prior to reading this specification. If the reader is building a TNC Server that supports IF-IMV, the reader is encouraged to read [6] prior to reading this specification.

1.2 Keywords

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in RFC 2119 [2]. This specification does not distinguish blocks of informative comments and normative requirements. Therefore, for the sake of clarity, note that lower case instances of must, should, etc. do not indicate normative requirements.

2 Background

2.1 Role of IF-M for SCAP

SCAP enjoys significant use in modern enterprises, with dozens of vendors integrating one or more of the SCAP component standards into their products. These products use SCAP to answer questions about an end system's configuration, patch level, installed products, and susceptibility to known vulnerabilities – all pieces of information about an endpoint that an enterprise might wish to know before allowing that endpoint access to the network, for targeting of additional sensors and mitigations, for detection of suspicious activity, or for other reasons. The use of TNC protocols to transport and encode the SCAP messages provides a valuable linkage between the TNC and SCAP communities.

As noted earlier, SCAP describes the coordinated use of a suite of standards. These component standards of SCAP include:

- Common Vulnerabilities and Exposures (CVE) [9] – an enumeration of unique identifiers for publicly known security vulnerabilities
- Common Vulnerability Scoring System (CVSS) [14] – a metric to assign a score to software vulnerabilities to help users prioritize risk
- Common Configuration Enumeration (CCE) [12] – an enumeration of security-relevant configuration elements for applications and operating systems
- Common Configuration Scoring System (CCSS) [16] - a metric to assign a score to security-relevant configuration elements to help users prioritize responses
- Common Platform Enumeration (CPE) [13] – a structured naming scheme used to identify information technology systems, platforms, and packages
- Open Vulnerability Assessment Language (OVAL) [10] – a language for making logical assertions about the state of an endpoint system
- Open Checklist Interactive Language (OCIL) [15] – a language to provide a standard way of querying a human user
- eXtensible Configuration Checklist Description Format (XCCDF) [11] - a language to express, organize, and manage security guidance
- Asset Reporting Format (ARF) [17] - a language to express information about assets

It is not necessary to understand the details of these specifications to implement the SCAP Messages for IF-M specification, and it is beyond the scope of this specification to discuss the details of these individual standards. If more information about individual SCAP component specifications is desired, please see the noted references for information.

Many products use the SCAP standards to manage assessments of end systems. Commonly, SCAP assessment instructions are transmitted from some assessment server to the end system, which then performs the required assessment and returns the results to the server. The exact means of transmitting this information between server and client is, however, not provided in the SCAP specifications. The SCAP specification only covers the expression of assessment instructions and how those assessment instructions are used to guide an assessment; the communication of the assessment instructions between server and client, as well as how the results are used, are beyond the scope of SCAP. As such, vendors with SCAP products today have defined their own methods of transmitting SCAP content and triggering assessments.

The SCAP Messages for IF-M specification describes a standard way to communicate SCAP assessment instructions and results between servers (IMVs) and clients (IMCs) within the IF-M protocol at the top of the TNC architecture. Defining such a standard within the TNC architecture has two specific advantages. First, it allows SCAP assessments to occur as part of the regular TNC exchanges. TNC supports assessment of an endpoint prior to that endpoint's establishment of a connection to a network as well as re-assessment at any time after this connection. The SCAP Messages specification allows SCAP to be used in making such assessments. Secondly, by providing a standard way of exchanging SCAP content between servers and clients, this specification helps support interoperability between the products of different vendors. It should be emphasized that there is no expectation that vendors will abandon the existing communication mechanisms they currently use when communicating between servers and clients that are both of their design - in fact, this specification specifically allows such communication mechanisms to be used when available. However, when communicating between endpoints that may not understand the same proprietary protocols, this specification provides a simple standard that allows basic SCAP assessments to be managed and performed.

2.2 Supported Use Cases

This section describes the SCAP Messages for IF-M use cases that must be supported. The primary usage of SCAP over the IF-M interface is to enable the challenger (e.g. TNC Server) to initiate and iteratively send a series of one or more queries to obtain measurement information about the attested system (e.g. TNC Client) in a manner compatible with the SCAP standards. A large number of vendor tools already support assessments using the SCAP standards; the SCAP Messages for IF-M use cases reflect this specification's intent to make it easier for SCAP tools to integrate into the TNC architecture.

Similar to the TLV [7] and PTS Protocol [8] bindings for IF-M, SCAP can be used to identify the system artifacts to be collected and/or evaluated during an assessment. It does this by identifying specific system artifacts (registry keys, files, modules, etc.) to query and/or expected values for these entities. SCAP is also capable of encapsulating the results of these evaluations. Throughout this specification, we will refer to the former as "SCAP assessment instructions" and the latter as "SCAP results". The term "SCAP content" will be used for either of these cases.

The use cases that must be supported by SCAP products when integrated with TNC can be grouped into three general usage categories: Provisioning, Assessment, and Freshness. Each category describes multiple alternatives related to that category. Any combination of these three usages should be supported by this specification.

2.2.1 Provisioning

Provisioning deals with the manner in which the set of SCAP assessment instructions are conveyed to the endpoint. In much the same way as IF-M includes a Component (IF-M) Subtype identifying the part of the target system to be measured and the desired information, SCAP assessment instructions describe what aspects of the system need to be evaluated as part of the TNC assessment.

In this protocol, SCAP content is ultimately pushed from an IMV to an IMC. For a given assessment (i.e., a given run of this protocol) the content in question may either be pushed from an IMV or it might already be resident on the IMC in a cache of previously received content. The protocol is designed to account for either of these situations.

2.2.2 Assessment

SCAP assessment instructions can guide assessments not only by identifying the relevant system artifacts that should be measured, but also by indicating the acceptable settings of these artifact measurements. SCAP results are often extremely detailed, but very verbose. Sometimes this level of detail is needed in order to collect details about the actual configuration of an assessed platform. Other times, it is simply necessary to verify that the platform meets a minimum set of requirements without going into detail as to how it does so. The SCAP Messages protocol supports both of these scenarios by allowing the IMV to control the nature of the assessment results returned by the IMC. These results can range from detailed SCAP results documenting a range of system artifacts, to minimal summaries of where the platform met or failed to meet a set of requirements, to simple binary results indicating that the system passed or failed a set of tests.

2.2.3 Freshness

SCAP assessment instructions can encapsulate large policies that are time consuming for a client to assess. As a result, it is sometimes desirable for a client to perform a self-initiated assessment at some time when it will be less disruptive to regular use and then store the corresponding SCAP results for later use. To support this idea, the TNC Server may indicate a minimum freshness level for the TNC Client's cached SCAP results. If, for a given set of assessment instructions, the client has a stored copy of SCAP results from an assessment more recent than the given freshness, then those SCAP results can be returned without initiating a new assessment on the client. If there are no SCAP results corresponding to the requested set of assessment instructions, or if existing results are older than indicated by the freshness value in the TNC Server's query, then the TNC Client must either initiate a new assessment and return the resulting SCAP results or return an error message if the desired assessment cannot or should not be initiated.

2.2.4 IF-M Use Cases

SCAP messages for IF-M are intended to operate over the IF-M interface and, as such, are intended to meet the use cases set out in the IF-M specification. In particular, SCAP messages for IF-M must support cases where the TNC Client determines that an assessment of the endpoint is required and invokes one or more IMCs to send measurements to their corresponding IMVs on the TNC Server. Likewise, SCAP messages for IF-M should also support cases where the TNC Server initiates assessment, invoking one or more IMVs to send requests to their corresponding IMCs on the TNC Client.

2.3 Non-supported Use Cases

Several use cases, including but not limited to these, are not covered by this version of SCAP Messages for IF-M:

- TNC components are not expected to be able to convert non-SCAP content into SCAP content or vice versa. While some tools may wish to provide translations as a way to bridge TNC components that support SCAP with other TNC components that do not support SCAP, this is not a requirement.
- There are many vendor products that support SCAP today and are capable of receiving SCAP assessment instructions, performing assessments, and returning SCAP results. While the SCAP content exchanged in SCAP messages for IF-M follows the same standard used by these products, this specification is not intended to support automated interaction between TNC components and software components that were not intended to interoperate with TNC. Instead, this specification provides another means of communicating assessment information within the TNC architecture. It does not describe procedures for the interaction of TNC and non-TNC components.
- While SCAP allows a great deal of interoperability between SCAP supporting tools, it is not always the case that two SCAP vendors will format results in an identical manner. Many fields are optional or are allowed to contain vendor-specific structures to allow for extensibility and flexibility in SCAP content. TNC implementations are not expected to resolve such misalignments. This specification is not intended to provide greater compatibility when exchanging content between two SCAP compatible tools than could be achieved through SCAP alone.
- This specification includes functionality based on an assumption that IMCs may contain caches of SCAP content. Management of any such caches will be important to maximize IMC efficiency. However, it is beyond the scope of this specification to define how the IMC caches will be managed. Implementers of IMCs and IMVs that support SCAP messages may use their own mechanisms to manage any content caches an IMC may have.
- Many SCAP vendors have already developed client-server architectures for providing a targeted device with SCAP assessment instructions, triggering assessments, and collecting results. In many cases, these architectures include features beyond basic SCAP assessment,

sometimes including non-SCAP-based testing, dynamic and fine-grained content control, and follow-on actions based on the results of these assessments. The SCAP Messages for IF-M specification is not intended to address these added capabilities but instead focuses on basic SCAP assessments.

2.4 Requirements

Here are the requirements that the SCAP Messages for IF-M specification must meet in order to successfully play its role in the TNC architecture. These parallel the IMV [7] and PTS Protocol [8] bindings for IF-M requirements, since they play the same role in the architecture and may be expected to operate concurrently during an assessment.

- Flexibility

  The SCAP Messages for IF-M must support all the functions and use cases described in the TNC architecture as they apply to the communications of SCAP content within TNC. The protocol defined in the SCAP Messages for IF-M specification must allow either the SCAP IMC or IMV to initiate the assessment or reassessment when operating over a usable IF-TNCCS session. When the IMC initiates the assessment, the IMV must allow the IMC to proactively send measurements prior to the IMV sending a measurement request.

  The SCAP Messages for IF-M protocol must be capable of supporting multiple round trip message exchanges during an assessment or reassessment. This allows the SCAP IMVs to send multiple requests for measurements potentially based on the results of earlier requests (e.g. based on the endpoint's operating system).

  SCAP Messages for IF-M must be capable of containing a wide variety of types of data values including: binary data, encrypted or compressed data, and textual strings as supported by the SCAP standards. Any string included in IF-M intended for user display must be able to be encoded in the user's preferred language, when known. IF-M must be able to carry standard defined attributes and/or vendor-defined attributes.

- Efficient

  The TNC architecture enables delay of network access until the endpoint is determined to not pose a security threat to the network based on its asserted integrity information. To minimize user frustration, the SCAP Messages for IF-M should minimize overhead delays and make IF-M communications as rapid and efficient as possible. This is a special challenge when dealing with SCAP as SCAP content tends to be very large. As such, mechanisms must be provided to allow assessments to occur without necessarily transmitting the full SCAP content itself.

  Efficiency is also important when you consider that some network endpoints are small and low powered, some networks are low bandwidth and/or high latency, and some IF-T protocols, or their underlying carrier protocol, might allow one packet in flight at a time or only one roundtrip. However, when the underlying IF-T protocol imposes fewer constraints on communications, this protocol should be capable of taking advantage of more robust communication channels (e.g. using larger messages or multiple roundtrips).

- Extensible

  SCAP Messages for IF-M must be very extensible allowing for additional SCAP content formats and values to be defined by future specifications and still be carried by IF-M.

- Scalable

The SCAP Messages for IF-M protocol must be capable of supporting a large number (hundreds) of measurements or results in a single message exchange and allow for use of attributes with large attribute values (tens of megabytes). This capability might not be practical or even necessary for all deployments (e.g. low bandwidth, high latency, time sensitive environments) but should be possible without alteration of the base protocol. Different exchanges have been defined to support different IMV and IMC capabilities and conventions as well as different possible bandwidth constraints.

- Interoperable

  This specification defines the protocol for how IMCs and IMVs can exchange and use SCAP content to perform assessments. Therefore a key goal for this specification is ensuring that all SCAP IMCs and IMVs, regardless of the vendor who created them, are able to interoperate in their performance of these duties.

2.5 Non-Requirements

There are certain requirements that the SCAP Messages for IF-M specification explicitly is not required to meet. This list may not be exhaustive.

- End to End Confidentiality

  SCAP content has no inherent mechanism for confidentiality, nor is confidentiality automatically provided by IF-M interface use. Should users wish confidentiality of assessment instructions or results, this must be provided at another level.

- Connectivity to Internet

  SCAP content can be written with remote references, requiring the interpreting software to follow URIs to collect information from other parts of the Internet. In a TNC exchange, where the client may not yet have broad connectivity, such a use would be problematic. As such, we explicitly note that, for compliance with SCAP messages for IF-M, the assessing client is not required to have network access to remote repositories. This includes remote copies of XML schemas and remote lookup of information from public dictionaries and databases. Instead, TNC clients must be able to receive all necessary information directly from the TNC server.

2.6 Assumptions

Here are the assumptions that SCAP Messages for IF-M makes about other components in the TNC architecture.

- Reliable Message Delivery

  The TNC Client and TNC Server are assumed to provide reliable delivery for IF-M messages and therefore the SCAP Messages sent between the SCAP IMCs and the IMVs. In the event that reliable delivery cannot be provided, the TNC Client or TNC Server is expected to terminate the connection.

2.7 SCAP Messages for IF-M Message Diagram Conventions

This specification defines the syntax of the SCAP Messages for IF-M using diagrams. Each diagram depicts the format and size of each field in bits. Implementations MUST send the bits in each diagram as they are shown from left to right for each 32-bit quantity traversing the diagram from top to bottom. Multi-octet fields representing numeric values must be sent in network (big endian) byte order.

Descriptions of bit fields (e.g. flags) values are described referring to the position of the bit within the field. These bit positions are numbered from the most significant bit through the least significant bit, so a one octet field with only bit 0 set has the value 0x80.

3 Design Considerations

This section discusses some of the key design considerations for the SCAP Messages for IF-M specification.

3.1 Flexible Content Structure Support

SCAP and its component standards remain subjects of ongoing development. The SCAP specification itself is revised regularly, and the component standards undergo revisions at varying intervals. As such, any message transporting SCAP information that is intended to support current SCAP content must include additional metadata indicating the SCAP version that is being conveyed. SCAP component languages and versions are identified using strings rather than using an enumerated list of values because, as SCAP evolves, any such list would rapidly become obsolete. By using the more verbose, but more flexible, option of identifying languages using strings, this specification can immediately support new SCAP languages and new versions of languages when they are released.

3.2 Non-divergence from Existing SCAP Practices

Many vendors have utilized SCAP, or at least component standards from it, in their products for over a decade. As such, there is a large existing investment in software and infrastructure, both by those vendors and by consumers who have purchased their products, in SCAP implementations. It is important that compliance with this specification does not require practices that diverge significantly from those currently surrounding SCAP use. SCAP vendors will have little interest in integrating their existing infrastructure with the TNC architecture if such integration requires a wholesale redevelopment of their software.

To ensure alignment, this specification is designed to be both minimal and modular. In the former respect, this specification focuses on the most basic procedures of an SCAP assessment: providing assessment instructions to the client and receiving results in return. In this way the specification attempts to focus on capabilities that will be covered by all existing SCAP implementations without forcing implementers to design significant new features. The modular approach is designed to address the fact that vendor implementations will usually support features beyond what are described in this specification and therefore may wish to use their own proprietary techniques to perform certain steps of the assessment process. Since the protocol defined in this specification is modular, if the vendor has a more powerful, proprietary means of interacting with an IMC for certain steps of the assessment process, the vendor can use their proprietary method of performing those steps and use the IF-M-based methods described in this specification for others. When the vendor does not have a proprietary method of interacting with an IMC (for example, if the IMC was developed by a different vendor) they can fall back to using just the universal exchanges described in this specification. In this way, this specification allows cross-vendor compatibility, without forcing vendors to sacrifice functionality.

3.3 Interoperation

As noted above, compatibility, especially when IMVs and IMCs are developed by different vendors, is central to the existence of this specification. It is therefore vital that the specification be clear on all points with regard to how to support the described interchanges. In particular, any exchanges between IMVs and IMCs must be well defined even if there are vendor proprietary communications before or after those exchanges. Towards this end, while IMCs and IMVs are not prohibited from interacting with external applications using vendor-proprietary protocols, the IMC-IMV exchanges over IF-M MUST only use the messages described in this specification and any malformed messages (i.e., messages that do not conform to this specification) over IF-M must be rejected.

4 SCAP Messages for IF-M Specification

This section describes the format and semantics of the SCAP Messages for IF-M protocol leveraging the existing SCAP specifications. SCAP Messages for IF-M uses the standard IF-M message header format. See the IF-M: TLV Binding specification [7] for information on this header format.

4.1 IF-M Subtype (AKA IF-M Component Type)

The TNC IF-TNCCS protocol provides a general message batching protocol capable of carrying one or more IF-M messages between the TNC Client and TNC Server. When IF-TNCCS is carrying an IF-M message, the IF-TNCCS message headers contain a 32 bit identifier called the IF-M Subtype. The IF-M Subtype field indicates the type of component associated with all of the IF-M messages carried by the IF-TNCCS message. The core set of IF-M Subtypes are defined in the IF-M specification. In order for the TNC protocols to carry SCAP messages, this specification adds the following enumeration element to table in section 4.4 of the IF-M specification [7] using the TCG Standard name space (SMI Private Enterprise Number 0x005597):

IF-M Subtype Component Type Name	TNC Standard Component Definition	Description
SCAP Messages	0x00000002	Software associated with SCAP-IMC supporting the SCAP Message binding to IF-M protocol.

Table 1 - IF-M Subtype

Architecturally, each TNC Client supporting SCAP Messages includes a component known as the SCAP-IMC that will receive messages sent with the SCAP Messages component type. The SCAP-IMC is an IMC that is responsible for receiving IF-M messages destined for SCAP-compatible assessment tools. The SCAP-IMC also sends the responses back to the TNC Server. Similarly, the SCAP-IMV exists on the TNC Server and is responsible for interpreting responses and making policy decisions based upon the received information. Each IF-M message described in this specification is intended to be sent between the SCAP-IMC and SCAP-IMV, so will be carried in an IF-TNCCS message indicating an IF-M Subtype of SCAP Messages. The attributes defined in this specification are not envisioned to be applicable to other types of IMCs (i.e., other IF-M Subtypes). Uses of the IF-TNCCS protocol MUST always include the SCAP Messages Subtype defined in this section when carrying the SCAP Messages over IF-M.

4.2 IF-M Message Header

The SCAP Messages for IF-M protocol described in this specification is an extension of the IF-M protocol described in the TNC Architecture. IF-M was designed to be very flexible to carry a wide variety of types of IF-M attributes (e.g. Product Information) that pertain to an enumerated set of component types (e.g. Firewall). IF-M attributes may be carried from IMC to IMV or vice versa and may carry information about state or other messages to be sent between an IMC and an IMV. Therefore the SCAP Messages for IF-M specification is largely a collection of attribute definitions relevant to the SCAP-based assessment of the system.

Figure 2, reproduced from the IF-M specification, shows the format of an IF-M attribute TLV. Multiple IF-M attributes can be sent in a single IF-TNCCS message, each housed within an attribute TLV.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Flags     |           Attribute Type Vendor ID            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Attribute Type                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Attribute Length                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Attribute Value (Variable Length)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2 - IF-M Attribute Format

TLV Field	Description
Flags	This field defines flags affecting the processing of the SCAP Messages for IF-M. Permissible flags are given in the IF-M specification. [7]
Attribute Type Vendor ID	This field indicates the owner of the name space associated with the Attribute Type - in this case, SCAP Messages for IF-M. Because this attribute type is defined within a TCG specification, this value must be the TCG SMI Private Enterprise Number value (0x005597).
Attribute Type	This field defines the type of the attribute. The values corresponding to SCAP messages are given in Table 3.
Attribute Length	This field contains the length in octets of the entire Attribute, including the Attribute's header.
Attribute Value	This field contains the SCAP Message.

Table 2 - Fields of the IF-M Attribute Format

4.3 SCAP Message Exchanges

This section discusses the envisioned message exchanges necessary to perform an SCAP-based attestation. There are seven defined messages in this specification, each used in specific sets of exchanges. This section outlines the supported exchanges, noting the expected message flow and the intent of the particular exchange.

The messages defined in this specification appear below with a short summary of their purposes. Each message is described in greater detail in subsequent sections.

- **SCAP References Message** - This message is used to request that an IMC indicate its capabilities, including which SCAP assessment instructions the IMC has cached. It is always sent from an IMV to an IMC.
- **SCAP Capabilities and Inventory Message** - This message is used to indicate the SCAP languages and versions supported by an IMC as well as a list of SCAP assessment instructions the IMC has cached locally. It is always sent from an IMC to an IMV.
- **SCAP Content Message** - This message is used to send actual SCAP assessment instructions. These messages are almost always fairly large and thus unlikely to be usable in restricted bandwidth environments, such as 802.1X exchanges. It is always sent from an IMV to an IMC.
- **SCAP Assessment Message** - This message is used to initiate or indicate the initiation of an SCAP assessment. Depending on the exchange, it might be sent either by an IMV or an IMC - see section 4.3.5 for examples.

- **SCAP Results Message** - This message contains the SCAP results of an SCAP assessment. These messages are almost always fairly large and thus unlikely to be usable in restricted bandwidth environments, such as 802.1X exchanges. It is always sent from an IMC to an IMV.
- **SCAP Summary Results Message** - This message contains a summary of the results of an SCAP assessment using bandwidth-minimizing encoding. It is intended to provide results in restricted bandwidth environments or in cases where the full details of SCAP result structures are not needed. It is always sent from an IMC to an IMV.
- **SCAP Error Message** - This message indicates that a fatal error was encountered during an SCAP message exchange. It is not included in any of the exchange diagrams listed below, but instead may be sent by an IMC at any time to indicate that an unexpected problem relating to the message exchange was encountered. It is always sent from an IMC to an IMV; the IMC MUST always terminate the message exchange after an SCAP Error Message is sent. If the IMV experiences a fatal error, it simply closes its connection to the IMC and does not need to provide any reason for doing so, in which case the IMC MUST accept the termination of the exchange without error.

Some SCAP content is unlikely to change frequently. For example, a platform's CPE dictionaries would be relatively static. Some exchanges are written to utilize client caching to minimize the amount of information that must be exchanged between the IMV and IMC. Some exchanges become infeasible over low-bandwidth connections, such as 802.1X, if the IMCs do not have access to cached copies of relevant content.

4.3.1 Vendor Proprietary Exchanges vs. SCAP Message Exchanges

Most existing SCAP vendors already have a client-server architecture which they use to perform assessments of endpoints, managed by some central service. As such, most vendors already have defined their own exchanges for provisioning endpoints with SCAP content, initiating assessments, and collecting results. Vendor proprietary protocols MAY be used to manage an IMC or IMVs' state, but MUST NOT allow a vendor proprietary protocol to change its state in the middle of an SCAP Message exchange.

The SCAP Messages for IF-M specification defines three exchanges:

- Capabilities exchange, in which the IMV discovers the existing capabilities of an IMC, including what SCAP assessment instructions the IMC may have cached
- Content exchange, in which the IMV provides SCAP assessment instructions to the IMC
- Assessment exchange, in which assessment results are requested and subsequently provided by an IMC

A vendor's proprietary protocol may have capabilities to support the objectives of any or all of these exchanges. Moreover, those vendor protocols may support features beyond the basic SCAP assessment scenarios supported by the SCAP Messages for IF-M specification. Because of this, vendors may prefer to use their own proprietary protocols when interacting with their own clients in situations outside of a TNC session.

In order to be compliant with the SCAP Messages for IF-M specification, an IMC or IMV MUST support the Capabilities Exchange and the Assessment Exchange. They SHOULD support the Content Exchange; however, some vendors may require all content on their SCAP endpoint assessment clients, which correspond to IMCs, to be controlled from their own central server and may wish to prohibit any other parties from altering the cached assessment instructions on their clients. For this reason, they may choose not to support the Content Exchange on their IMC, since such an exchange could be initiated by any compliant IMV, not just their own server. In short, to be considered compliant with this specification, an IMC must be able to report its capabilities and cached assessment instructions and must be able to initiate and return results from an assessment, all by using exchanges defined by this specification. However, such an IMC is NOT required to use the exchanges defined in this specification to update its supply of cached assessment instructions.

Vendors are, however, encouraged to support the Content Exchange in both their IMV and IMC implementations. Supporting this exchange allows a greater degree of interoperability to be achieved within an enterprise, as it allows all basic activities necessary for an SCAP assessment to occur using standard mechanisms.

4.3.2 SCAP Content

The handling of SCAP content is central to any discussion of SCAP use - in fact, the SCAP specification itself is primarily devoted to formatting and interpretation of SCAP content. This section provides an outline as to how SCAP content is treated within this specification.

4.3.2.1 Documents, URIs, and SCAP Content

This specification makes frequent mention of SCAP content "documents". Specifically, the messages defined herein identify content by a URI and will often use an MD5 as well, which is intended to be a hash of a given document. SCAP content contains references that are built around the concept of documents. For example, an XCCDF Benchmark is usually represented as a single XML document. It can contain references to OVAL and OCIL checks, and these checks contain the URIs of documents where these checks can be found. As such, the concept of "documents" containing SCAP content, usually formatted in XML, is an inherent part of SCAP use. Likewise, the use of URIs to identify these documents is also a standard practice within SCAP. As such, the conventions outlined in this specification conform to SCAP conventions.

This said, documents are not the only way to manage SCAP content. Most SCAP content can be broken down into smaller blocks. For example, XCCDF content can be broken down into Rules, Groups, and Profiles, while OVAL content can be broken down into Definitions, Tests, Objects, and States. These entities all reference other entities within the same block of content (i.e., a document) so are not necessarily usable in isolation, but they still represent meaningful units of information. Some vendors, rather than managing content through static documents, manage these smaller entities, dynamically generating new documents by selecting, mixing, and matching these smaller elements. However, before an assessment can be performed, the assessing device (endpoint) must have some understanding of what content belongs to a conceptual document and provide it with a URI so that references within the SCAP content can be resolved. As such, the concept of a document and its URI should be familiar to all vendors regardless of their individual content management procedures.

The messages defined in this specification do not support the exchange of SCAP content below the level of a document. In other words, one could not send an XCCDF Rule from an IMV to an IMC without sending an entire XCCDF document, nor is there any requirement for an IMC to dynamically generate new documents composed from smaller blocks of content it received. This may allow for less fine-grained control of SCAP content than a vendor might support using proprietary techniques. However, it does represent both a "least common denominator" for content management, since all SCAP tools at least need to be able to manage SCAP documents and since SCAP references require that named documents that appear within SCAP content be resolvable. Future revisions of this protocol may support content management at a finer level of granularity, but this initial release seeks to enable the broadest compatibility with existing SCAP implementations. As such, the use of the term "document" is used throughout this specification, even though the actual management of SCAP content via vendor-proprietary protocols might occur at a different level of granularity. Vendors that manage SCAP content at the sub-document level - for example, by dynamically composing smaller units - should associate a URI with this composition and should calculate an MD5 hash for this composition as if it was an actual document.

It should be emphasized that this specification does not constrain how SCAP content is stored on either an IMC or an IMV. SCAP documents might be stored on the appropriate device as files on the file-system, which is a common practice in SCAP, but they might be stored in other ways as well. Documents can even be broken up into the aforementioned smaller blocks of SCAP content and stored in this way, so long as the original document can be reconstructed upon request so it can be used in assessments.

4.3.2.2 Associating Documents and URIs

As mentioned earlier, SCAP documents link to each other through a series of references written into the SCAP content. These references take the form of a URI to a document and sometimes the name of a particular sub-block within that document. These URIs can be absolute or relative, and can even point to remote resources. In many SCAP languages, these URIs are, in fact, intended as URLs in that they indicate the actual locations of resources which are pointed to in an SCAP reference.

The URIs that IMVs and IMCs associate with SCAP documents are simply labels that the IMV or IMC associates with a document. Since the IMV that sends SCAP content might not store its content in the same way as the IMC that receives it, the URI cannot be assumed to provide any location information with regard to the content. As such, the URI is an identifier, but not a locator (i.e. it is not a URL). In fact, the URI could look like a reference to a remote resource (e.g., "http://oval.mitre.org/rep-data/5.10/org.mitre.oval/i/platform/red.hat.linux.9.xml"), but the IMV and IMC would still treat this only as a label associated with a provided document rather than a pointer to some remote file.

When an IMC performs an assessment, it SHOULD resolve all references within SCAP content by treating the URIs in those references as identifiers to SCAP documents it has received that are labeled with identical URIs. In other words, the URLs in the SCAP content are used as URIs in the IMCs and IMVs and instead of being resolved to a particular location, are used to identify named documents on the IMC or IMV. As such, while the URI's that IMVs and IMCs assign to SCAP documents cannot be assumed to represent meaningful locations, they should still be selected carefully as those URIs will be used to resolve the references that appear within SCAP content. This would be why one might wish to associated a document with a URI that looks like a reference to a remote resource, such as shown in the previous paragraph - if the given document was pointed to by the remote URL in the SCAP content, that document should be named using an identical URI in the IMV-IMC exchanges so the reference can be resolved.

Because there may be multiple parties providing SCAP content to an IMC, URI collisions are a possibility. The protocol described in the following sections does provide ways for IMVs to detect if the content associated with a particular URI differs from their expectations (see section 4.6, which discusses the SCAP Capabilities and Inventory Message) so even during URI collisions it is always clear what content was actually used in an assessment. However, when there are collisions the IMV may need to re-provision the IMC with the desired content before desired results can be obtained. To avoid collisions in the first place, IMVs MAY wish to include some identifying information unique to that IMV in all URIs that IMV publishes. For example, an IMV could turn all URIs into absolute references pointing to the IMV. (E.g., "winxp.xml" might become "http://imv-name-123.company-name-456.com/scap-content/winxp.xml".) As noted earlier, an IMC would use this value as an identifier rather than a locator so IMVs would not actually need to be able to respond to requests to the given URI as a URL. Such a URI would, however, significantly reduce the chance of URI collisions with other content providers. Of course, the SCAP references in all associated content would also need to be changed to match the modified URI so SCAP references could resolve correctly on the IMC. Since changing content is not always possible (e.g., content created by third parties and then digitally signed to preclude modification), other schemes to prevent URI collisions might be necessary.

Note that, an IMC MAY choose to resolve an SCAP reference using the actual location given in the reference's URI (i.e., treat it as a URL), but if the location cannot be resolved (e.g., due to network failure) the IMC cannot report the resource as unreachable unless it also has determined that it has no cached document with the corresponding URI. In other words, the IMC has the option to resolve SCAP references using the normal URL-resolution that most SCAP tools use today, but references cannot be treated as unresolvable until the IMC has tried to resolve the reference using its cache. Of course, contacting remote repositories outside the control of the enterprise can potentially lead to security risks. See section 5.2.4 for a discussion of this.

4.3.3 Capabilities Exchange

This exchange is used to inform the SCAP-IMV of the capabilities of the SCAP-IMC. In particular, from this exchange, the IMV learns which version of SCAP the IMC supports, which SCAP languages the IMC supports, and what, if any, cached SCAP assessment instruction documents are present on the IMC. This exchange might be used to precede a Content Exchange and/or an Assessment Exchange, if the IMV was unaware of the IMC's capabilities, or if it needed to determine what, if any, SCAP assessment instruction documents needed to be provided to the IMC before a suitable assessment could be performed.

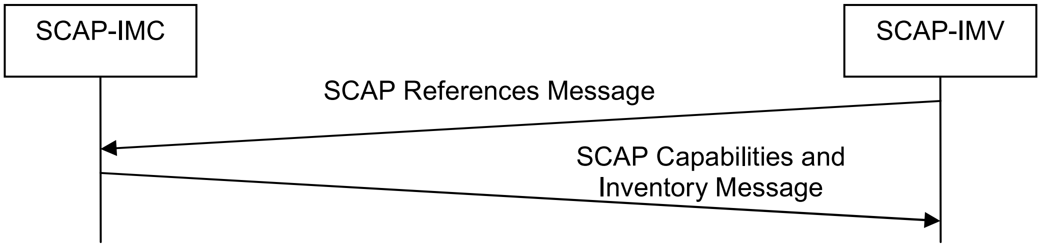


Figure 3 - SCAP Messages Capabilities Exchange (IMV-Initiated)

In this exchange, the IMV indicates to the IMC, via an SCAP References Message, what SCAP assessment instruction documents it is interested in. The IMC responds with a list of the SCAP languages it can support and which of the SCAP assessment instruction documents identified in the SCAP References Message it has cached. The inventory provided by the IMC represents the subset of the content identified by the IMV that the IMC has in its cache; the IMC MUST NOT include SCAP content the IMV did not identify.

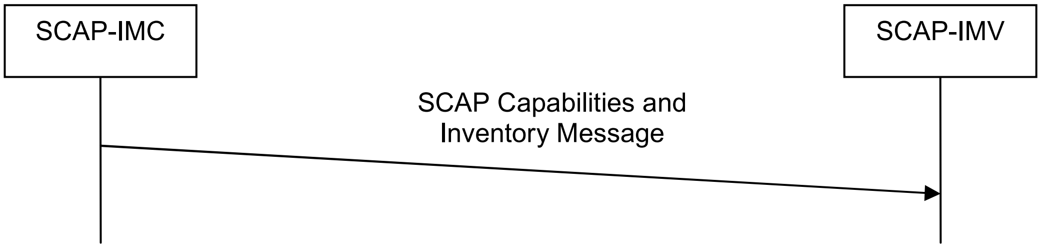


Figure 4 - SCAP Messages Capabilities Exchange (IMC-Initiated)

In a variation of this exchange, the IMC can initiate the exchange by sending the IMV an unsolicited SCAP Capabilities and Inventory Message. Since there was no preceding SCAP References Message, the IMC would nominally return a list of all of its cached assessment instruction documents. However, since an IMC on a long-running platform might have an extremely large collection of cached assessment instruction documents, a complete enumeration of them would lead to a very large message while providing little benefit, since some of the content may have become obsolete. We suggest that the IMC track the use of its cached SCAP assessment instruction documents and only identify documents anticipated to be of interest to the IMV, such as documents used within the last several assessments. The exact procedures by which an IMC determines what to list in its inventory are beyond the scope of this specification and are left to the IMC implementer. Note that the last-modification date of the documents may not be a good criterion for this selection, as some SCAP documents can be valid for a very long period of time.

All IMVs MUST support both versions (IMV-initiated and IMC-initiated) of this exchange. An IMC MUST support the IMV-initiated version of this exchange, but MAY choose not to support the IMC-initiated version.

4.3.4 Content Exchange

This exchange is used by the IMV to supply the IMC with necessary SCAP assessment instruction documents. In many cases, this exchange would follow a Capabilities Exchange, where the IMV learned that the IMC did not have a cached copy of some necessary documents. Alternatively, the IMV might spontaneously send assessment instructions to the IMC - this could happen because these were new assessment instruction documents and, therefore, the IMC could not have a cached copy.

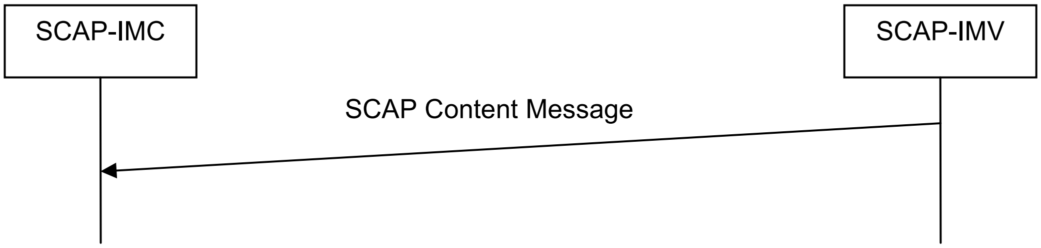


Figure 5 - SCAP Messages Content Exchange

This exchange simply consists of one or more SCAP Content Messages sent from the IMV to the IMC. The IMC is expected to update its cache of assessment instruction documents appropriately, as described in section 4.7.

As noted earlier, SCAP assessment instructions often contain references, and these references usually contain URIs. IMCs MAY treat the URIs within SCAP content as locations, possibly remote, of other content to consult. However, sometimes it is impossible for an IMC to resolve remote URLs, such as if the IMC is attempting to perform an assessment before its client has been granted network access. For this reason, IMVs will usually want to provide IMCs with all content needed to perform an assessment. This would mean, for a given SCAP assessment instruction document, the IMV would need to know what other documents that first document referenced. This might be discovered dynamically by searching for SCAP references or might be explicitly provided to the IMV when it is given a piece of content. If the IMV does not provide all documents necessary to resolve all needed references, the IMC might not be able to perform a given assessment.

All IMCs and IMVs SHOULD support this exchange. However, vendors may use proprietary protocols to manage the IMC's assessment instruction document cache instead of, or in addition to, using this exchange.

4.3.5 Assessment Exchange

In this exchange, the IMV initiates an assessment using an SCAP Assessment Message and the IMC responds with the appropriate results along with an SCAP Capabilities and Inventory Message to identify the SCAP assessment instruction documents used. The IMV makes the assumption not only that the IMC has a cached copy of all required assessment instruction documents, but also that the named SCAP documents in the IMC's cache are unchanged relative to the IMV's expectation as to their contents; these assumptions can be verified using the SCAP Capabilities and Inventory Message in the IMC's response. If the IMC lacks required SCAP documents, it will simply respond with an SCAP Error Message and terminate the exchange. If the IMC has access to all the referenced assessment instruction documents, but the contents of these documents differ the IMC's expectations, this will be evident in the SCAP Capabilities and Inventory Message from the IMC, since that message contains MD5 hashes of all documents used.

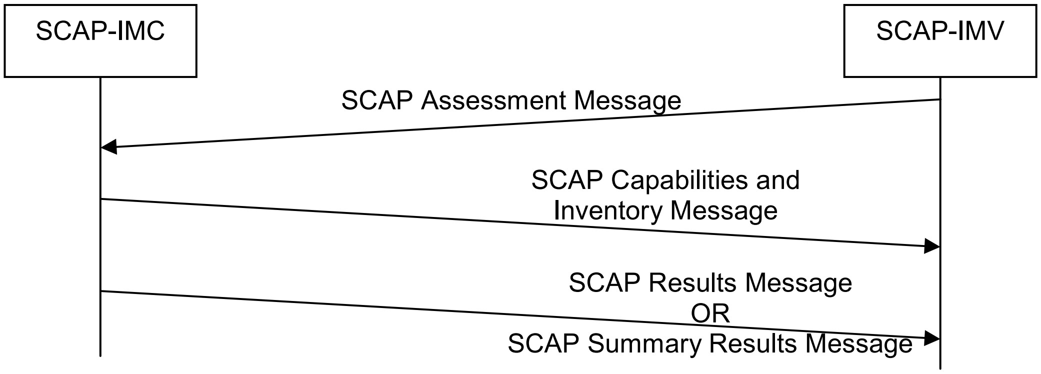

SCAP-IMC
SCAP-IMV
SCAP Assessment Message
SCAP Capabilities and Inventory Message
SCAP Results Message OR SCAP Summary Results Message

Figure 6 - SCAP Messages Assessment Exchange (IMV-Initiated)

This exchange begins with the IMV's SCAP Assessment Message, which identifies the root document of the SCAP assessment to perform and the type of expected results. The IMC performs the required assessment and identifies all assessment instruction documents required to perform the assessment, recording the URIs and the hashes of those documents. Note that SCAP assessment instruction documents that are referenced but not actually used in the assessment do not need to be recorded.

When the IMC's assessment is complete, it sends an SCAP Capabilities and Inventory Message back to the IMV. This message identifies the SCAP version and languages supported by the IMC, since this might have some impact on the results, as well as the URIs and hashes of all the SCAP assessment instruction documents used in the assessment. This is followed by the appropriate results message, using a format and message type as dictated by the SCAP Assessment Message.

It is recognized that most existing SCAP implementations assume that assessments will only occur using the desired SCAP assessment instructions because, in that vendor's implementation, those assessment instructions are strictly controlled by a single party. In the SCAP Messages for IF-M protocol, however, it is possible for multiple parties to influence an IMC's cache of SCAP assessment instructions. For this reason, the IMV SHOULD review the SCAP Capabilities and Inventory Message and verify that the assessment was performed using the expected SCAP assessment instructions.

There is also an IMC-initiated variant of this exchange. Such a version might be used if the IMC performed an assessment, possibly at a regular interval or at a time when the target machine was idle, and wished to apprise the IMV of the results. In this case, the exchange begins with an SCAP Assessment Message, but sent from the IMC to the IMV.

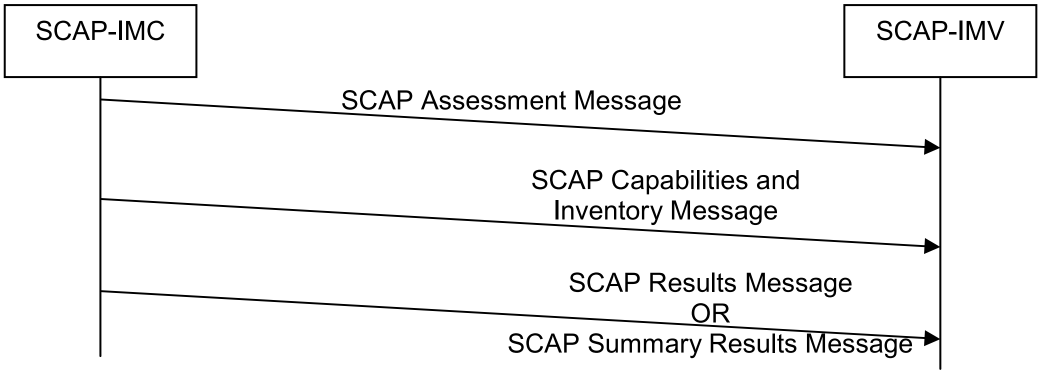

SCAP-IMC
SCAP-IMV
SCAP Assessment Message
SCAP Capabilities and Inventory Message
SCAP Results Message OR SCAP Summary Results Message

Figure 7 - SCAP Messages Assessment Exchange (IMC-Initiated)

The IMC's SCAP Assessment Message informs the IMV as to which SCAP assessment instruction document will form the root of the assessment and what sort of results to expect. The SCAP Capabilities and Inventory Message is used to identify all utilized SCAP assessment instruction documents (by URI and hash) that were used in this assessment, as described above. Finally, the appropriate results message, as indicated by the IMC's SCAP Assessment Message, is sent to the IMV with the assessment results.

All IMVs MUST support both versions (IMV-initiated and IMC-initiated) of this exchange. An IMC MUST support the IMV-initiated version of this exchange, but MAY chose not to support the IMC-initiated version.

4.4 SCAP Messages for IF-M Attribute Enumeration

The attributes defined in this section all use the TCG SMI Private Enterprise Number (0x005597) in the Attribute Type Vendor ID field of the IF-M Attribute Header described in Table 2. The following table briefly describes each attribute and defines the value to be used in the Attribute Type field of the IF-M Attribute Header.

Attribute Purpose	Attribute Name	IWG Standard Attribute Type	Description
Capabilities Exchange			
	SCAP References Message	0x00000001	Requests an IMC to report on its capabilities
	SCAP Capabilities and Inventory Message	0x00000002	Send language support information and identifiers for cached SCAP assessment instructions to an IMV
Content Exchange			
	SCAP Content Message	0x00000003	Send SCAP assessment instructions to an IMC
Assessment Exchange			
	SCAP Assessment Message	0x00000004	Send information about the initiation of an SCAP-based assessment
	SCAP Results Message	0x00000005	Send SCAP assessment results to the IMV
	SCAP Summary Results Message	0x00000006	Send a summary of SCAP assessment results to the IMV
Error			
	SCAP Error Message	0x00000007	Indicate a fatal error during some part of the SCAP Messages exchange.

Table 3 - SCAP Messages Attribute Enumeration

4.5 SCAP References Message

This message is sent from an IMV to an IMC to request that the IMC send a summary of its assessment capabilities. Content is identified by URI as well as an MD5 hash of the document. Per section 4.7, two distinct documents (i.e., documents with different MD5 hashes) MUST NOT have the same associated URI within the IMC's cache.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Reserved    |   Doc Count   |            URI Len            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    URI (Variable Length)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         MD5 Hash (16 Bytes)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         MD5 Hash                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         MD5 Hash                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         MD5 Hash                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 8 - SCAP References Message

Header Field	**Description**
Reserved	Reserved for future use. This field MUST be set to zero on transmission and ignored upon reception.
Doc Count	This field defines the number of document references present in this message. The URI Len, URI, and MD5 Hash properties will be repeated, in order, the number of times given in this field. This field allows a maximum of 255 documents to be included in this message.
URI Len	This field defines the number of octets in the URI string field.
URI	This field contains a UTF-8 string providing a URI for the provided assessment instructions. This is used to identify the assessment instructions to be used in the assessment.
MD5 Hash	This field contains an MD-5 hash of the referenced content.

Table 4 - SCAP References Message Fields

4.6 SCAP Capabilities and Inventory Message

This message is sent from an IMC to an IMV to indicate the version of SCAP it can support, the individual SCAP languages that it supports, and a list of cached SCAP assessment instruction documents. If this message is transmitted in response to an SCAP References Message from the IMV, then the list of document references in the SCAP Capabilities and Inventory Message will be those documents that are both in the IMC's cache and which were referenced in the SCAP References Message. As such, it represents the list of the SCAP content that is locally available and which is of interest to the IMV. Based on this response, the IMV can decide which, if any, SCAP content needs to be sent to the IMC.

If this message is the first message of an IMC-Initiated Capabilities Exchange, the list of SCAP documents represents the cached SCAP assessment instruction documents available to the IMC. It is recommended that, if the cached inventory is especially large relative to the constraints of the transport protocol, that this inventory list be truncated. How this list is truncated is beyond the scope of this specification.

If this message immediately precedes an SCAP Results Message or an SCAP Summary Results Message in an SCAP Assessment Exchange, then the message MUST list the SCAP assessment instruction documents used to create those results. In this case, the IMC MUST only list SCAP documents that are actually used - SCAP assessment instruction documents that are unused in the assessment, even if they appear in references, MUST be excluded. In this case, MD5 measurements MUST reflect the state of the documents at the time they are used for the assessment - cached hash values taken at some earlier time MUST NOT be used.

Note that the message conveys the supported version of SCAP but only the names for the supported SCAP languages even though those languages have their own version values. This is because each version of SCAP explicitly identifies the supported versions of each of its supported languages. As such, the individual language versions are implicit in the version of SCAP supported. Specifically, NIST's Derived Test Requirements for a given version of SCAP definitively state the versions of each component specification that must be supported to be compliant with that version of SCAP.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Reserved    |   SCAP Major  |  SCAP Minor   | Language Count|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Language Len          |   Language (Variable Length)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Doc Count   |            URI Len            | URI (Variable)|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         MD5 Hash (16 Bytes)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         MD5 Hash                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         MD5 Hash                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         MD5 Hash                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 9 - SCAP Capabilities and Inventory Message

Header Field	**Description**
Reserved	Reserved for future use. This field MUST be set to zero on transmission and ignored upon reception
SCAP Major	The major version of the version of SCAP supported by the IMC
SCAP Minor	The minor version of the version of SCAP supported by the IMC
Language Count	The number of languages specified in the message. The Language Length and Language fields will be repeated this many times, in order.
Language Len	This field defines the number of octets in the Language string field
Language	This field contains a UTF-8 string identifying one of the IMC's supported SCAP languages. This MUST be the XML namespace of the language.
Doc Count	This field defines the number of document references present in this message. The URI Len, URI, and MD5 Hash properties will be repeated, in order, the number of times given in this field. This field allows a maximum of 255 documents to be included in this message.

URI Len	This field defines the number of octets in the URI string field.
URI	This field contains a UTF-8 string providing a URI for the referenced SCAP content.
MD5 Hash	This field contains an MD-5 hash of the referenced content. No pre-processing should be done before the MD-5 hash is calculated - this should be the hash of the document exactly as it was received by the IMC.

Table 5 - SCAP Capabilities and Inventory Message Fields

4.7 SCAP Content Message

An SCAP Content Message is used to send SCAP assessment instructions from the IMV to the IMC. Specifically, it can contain one or more content "documents". As noted earlier, we use the term "document" to represent a bundle of SCAP content that would appear as a separate document on a file-system, even though they might be generated or stored by the IMV or IMC in other ways.

If the IMC's cache contains a document with the same URI and the same MD5 hash, the IMC MAY ignore that particular document in the SCAP Content Message and continue to use the version in its cache. If the IMC's cache contains a document with the same URI but with a different MD5 hash, the IMC MUST replace the old document in the cache with the new document provided by the message.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Reserved    | Content Count |           URI Len             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       URI (Variable Length)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Content Len                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Content (Variable Length)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 10 - SCAP Content Message

Header Field	**Description**
Reserved	Reserved for future use. This field MUST be set to zero on transmission and ignored upon reception
Content Count	This field defines the number of separate documents of SCAP content being sent. The URI Len, URI, Content Len, and Content fields are repeated, in order, the number of times given in this field.
URI Len	This field defines the number of octets in the URI string field.
URI	This field contains a UTF-8 string providing a URI for the provided content. Some SCAP content makes references to other SCAP content by its URI. The URI in this field is intended to be associated with content so that these references can be resolved. In other words, if some SCAP content makes reference to a URI 'foo.xml', and an SCAP Content Message associates the URI "foo.xml" with some set of content, then that SCAP reference should resolve to that content. All URIs within a set of assessment instructions must be unique relative to each other. A URI MUST be included even if there is no reference to the document by name in any SCAP content. URIs are case-insensitive within this message and within the IMC's cache.

Content Len	This field defines the number of octets in the Content string field.
Content	This field contains the actual SCAP content as a UTF-8 string. The message must be expressed as XML and must include an XML header. The content must validate against the appropriate schema(s), although actual validation by either the IMC or IMV is not required.

Table 6 - SCAP Content Message Fields

4.8 SCAP Assessment Message

This message, when sent from an IMV to an IMC, is used to request the results of a specific SCAP assessment. Those results might be created by an assessment that the IMC initiates in response to this message or could be cached results of the given SCAP assessment, providing those results are sufficiently fresh. When this message is sent from an IMC to an IMV, it is used to indicate the nature of the assessment whose results will immediately follow within the exchange.

The message contains several pieces of important information. First, it identifies the language and the version of the language for the assessment instruction document that forms the "root" of the assessment. Note: the version field contains the version of the identified language, not the SCAP version as would be provided in an SCAP Capabilities and Inventory Message. One can think of the content used in an SCAP assessment as a tree of references, with some documents referencing one or more other documents. However, all SCAP assessments have a root document that references other documents but is not itself referenced. For example, in an XCCDF-based assessment, the XCCDF document is the root document, and it references the OVAL, OCIL, and/or CPE dictionary documents that constitute the remainder of the assessment instructions. Because references are written into the SCAP content, identifying the root allows the remaining content to be identified unambiguously. Identifying the language and language-version of this root content indicates what type of SCAP tool is needed to execute the assessment. For example, if the root is an XCCDF document, then an interpreter that can process XCCDF content must be invoked.

In addition, the message contains 0 or more parameters to convey additional information about the processing of the SCAP content during the assessment. For example, an XCCDF Benchmark document is often invoked along with a Profile identifier in order to specify which XCCDF Profile should tailor the Benchmark prior to assessment. Parameters are used to convey this as well as other types of auxiliary information.

Finally, the message contains the URI of the root SCAP assessment instruction document and fields identifying the type of result that will be sent to the IMV. The result can range from complete SCAP results, which tend to be quite verbose, to a range of abbreviated summaries of these results. Depending on the value of these fields, the IMC will return either an SCAP Results Message or an SCAP Summary Results Message. Note that the only two result types that the IMC MUST support are "full results" (result type 0) and "absolute results" (result type 1). An IMC that supports the IMV’s requested result type MUST return that result type. An IMC that does not support the IMV’s requested result type MAY return a different result type. The IMC MUST, however, respect the IMV's request for summary results vs. regular results. For example, in the case where the IMV requests a result type that would be returned in an SCAP Summary Result Message but which is not supported by the IMC, the IMC MUST return results that still use an SCAP Summary Result Message. That is, the IMC cannot return full results to an IMV request for summary results or vice versa. Likewise, a request for full results MAY include a list of the SCAP result languages in which to record the assessment results. The IMC SHOULD make a best-effort to comply with this request, but MAY exclude some result languages if it does not support them and MAY add results in other languages. In an example of where the latter might occur, an IMV might request ARF results, but the IMC might not support ARF and might choose to send OVAL results instead. However, the IMC MUST NOT return summary results in response to a request for full results.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Reserved    |         Language Len          | Language (Var)|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Version Len  |           Version (Variable Length)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Param Count   | Parameter Type|         Parameter Len         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Parameter (Variable Length)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           URI Len             |  URI Label (Variable Length)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Result Type   |        Result Param Len       |Result Param...|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 11 - SCAP Assessment Message

<table>
<tr><th>Header Field</th><th>Description</th></tr>
<tr><td>Reserved</td><td>Reserved for future use. This field MUST be set to zero on transmission and ignored upon reception</td></tr>
<tr><td>Language Len</td><td>This field defines the number of octets in the Language string field</td></tr>
<tr><td>Language</td><td>This field contains a UTF-8 string identifying the SCAP language of the root content in this set of assessment instructions. This MUST be the XML namespace of the utilized language.</td></tr>
<tr><td>Version Len</td><td>This field defines the number of octets in the Version string field.</td></tr>
<tr><td>Version</td><td>This field contains a UTF-8 string identifying the version of the SCAP language of the root content in this set of assessment instructions. Trailing 0s (zeroes) in the version number MUST be dropped.</td></tr>
<tr><td>Parameter Count</td><td>Some types of SCAP assessments content require parameters. This section allows these parameters to be specified. This field defines the number of parameters associated with this message. The three fields of Parameter Type, Parameter Len, and Parameter are all repeated, in order, the given number of times. This might be 0 times if no parameters are needed.</td></tr>
<tr><td>Parameter Type</td><td>Available values for parameter type:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0</td><td>XCCDF Profile. The parameter field MUST contain the name of an XCCDF Profile to be used during the assessment</td></tr>
<tr><td>1</td><td>XCCDF Tailoring document. The Parameter field MUST contain the URI of an XCCDF Tailoring document. An XCCDF document with the given URI MUST be transmitted as part of this set of assessment instructions. The presence of this parameter MUST only occur when there is an XCCDF Profile identified by another parameter field and it names a Profile in the given Tailoring document.</td></tr>
<tr><td>2</td><td>OVAL External Variable document. The Parameter field MUST contain the URI of an OVAL variable document that should be used during an OVAL assessment. An OVAL Variable document with the given URI MUST be transmitted as part of</td></tr>
</table></td></tr>
</table>

	this set of assessment instructions. This parameter MUST NOT be supplied in combination with an XCCDF document, as XCCDF-based assessments generate their own OVAL Variable documents.
3	OVAL Definition List document. This document MUST contain a space-separated list of OVAL Definition ids. This parameter MUST NOT be supplied in combination with an XCCDF document, as XCCDF-based assessments generate their own list of OVAL Definition ids. When an OVAL Definition document is provided as the root of an assessment, by default every OVAL Definition in that document is directly processed. Providing a Definition List limits the processing of the OVAL Definitions to only those that appear in the Definition List. Note that OVAL Definitions can reference other OVAL Definitions and the presence of a Definition List does not prevent such references from being resolved, even if the referenced Definition is not in the Definition List. The Definition List only limits the OVAL Definitions that are directly executed in the assessment.
4	Oldest acceptable cached results. SCAP assessments can be time consuming. In order to reduce delays, IMV's MAY indicate that cached copies of corresponding assessment results are acceptable, if those cached results are more recent than a given time. If the IMC has cached results that are more recent than the supplied time, it MAY return these to the IMV without performing any additional assessment. If this parameter is not sent or if the IMC does not have cached results more recent than the given time, the IMC MUST either perform a new assessment or return an appropriate SCAP Error Message. The Parameter field MUST contain a date-time value expressed in ISO 8601 extended format [4].
5	OVAL Result Directives. OVAL defines a <directives> element that can be used to filter OVAL result documents. Specifically, this element can indicate that certain result values (e.g., true, false, error, not-applicable, etc.) should be omitted from OVAL result document created for an assessment. This element can also indicate whether OVAL result records with certain result values should be verbose ("full") or abbreviated ("thin"). The Parameter field MUST contain a single <directives> element from the OVAL Result Schema. Namespace abbreviations SHOULD NOT be used.

All other parameter type values are reserved for future use and MUST NOT be used in messages.

Parameter Len	This field defines the number of octets in the Parameter string field
Parameter	This field contains a UTF-8 string with a parameter value. The nature of this value is indicated by the Parameter Type field.
URI Len	This field defines the number of octets in the URI string field.
URI	This field contains a UTF-8 string providing the URI of the root content in this set of assessment instructions.

<table>
<tr>
<td>Result Type</td>
<td>This field indicates the type of the result being returned. Different SCAP languages express assessment results in different ways, and this field allows the nature of the results to be identified. Available result types are:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0</td><td>Full results. The IMC will return one or more SCAP documents detailing the findings of the assessment. This result type may have a result parameter representing a list of the language(s) in which to express the results. These appear as a space-separated list of XML namespaces for the relevant result languages. Note that in some SCAP component languages (e.g., XCCDF and OCIL) the result schema is identical to the assessment instruction schema, while in other languages (e.g., OVAL) there are separate schemas for assessment instructions and results. In the latter case, the given XML namespaces would be for the appropriate result schemas. The IMC SHOULD provide results using all of the listed languages. The IMC MAY omit results requested in a language it does not support and MAY include results expressed using other languages.</td></tr>
<tr><td>1</td><td>Absolute result. The assessment passes if every check in the root document of the assessment instructions evaluates to a value of "true" or "pass" (as appropriate for each individual language), regardless of the language in which that root content is expressed. The returned result will either hold "0" (fail) or "1" (pass). The Result Param Len field MUST be set to 0 for this Result Type.</td></tr>
<tr><td>2</td><td>XCCDF scoring model. The result for this assessment will be a numeric value computed using one of the XCCDF scoring models. This type has an additional result parameter value that MUST hold the URI of the XCCDF scoring model, as provided in the XCCDF specification, used to calculate the result. Vendor-defined scoring models MUST NOT be used.</td></tr>
<tr><td>3</td><td>XCCDF Rule list. The result for this assessment will be a comma-separated list of Rule-id/result pairs. The Result Param Len field MUST be set to 0 for this Result Type.</td></tr>
<tr><td>4</td><td>OVAL Definition list. The result for this assessment will be a comma-separated list of OVAL Definition id/result pairs. The Result Param Len field MUST be set to 0 for this Result Type.

Note that if XCCDF assessment instructions served as the root of this assessment, it is potentially possible for a single OVAL Definition to be executed multiple times with different variables, resulting in different results each time it is executed. The structure of this Result Type cannot differentiate such results. Therefore, this Result Type MUST only be used when the OVAL Definition document itself is the root content of the assessment.</td></tr>
<tr><td>5</td><td>OCIL Questionnaire list. The Result field for this assessment is a comma-separated list of OCIL</td></tr>
</table>
</td>
</tr>
</table>

	Questionnaire id/result pairs. The Result Param Len field MUST be set to 0 for this Result Type. All other result type values are reserved for future use and MUST NOT be used in messages. The type of the result SHOULD reflect the language of the root content of the assessment.
Result Param Len	This field defines the number of octets in the Result Param string field.
Result Param	This field contains a UTF-8 string providing a parameter used to interpret the result of the assessment. The contents of this field depend on the Result Type field.

Table 7 - SCAP Assessment Message Fields

4.9 SCAP Results Message

This message is used to send complete SCAP results from the IMC to the IMV. Complete SCAP results may consist of multiple documents. These documents can be quite large, so this message should only be used over connections with sufficient bandwidth. This message MUST only be used if the preceding SCAP Assessment Message dictated that the IMC return full results.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Reserved    | Content Count |            URI Len            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      URI (Variable Length)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Language Len          |   Language (Variable Length)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Version Len  |           Version (Variable Length)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Content Len                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Content (Variable Length)                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 12 - SCAP Results Message

Header Field	Description
Reserved	Reserved for future use. This field MUST be set to zero on transmission and ignored upon reception
Content Count	This field defines the number of separate documents of SCAP content being sent. The URI Len, URI, Language Len, Language, Version Len, Version, Content Len, and Content fields are repeated, in order, the number of times given in this field.
URI Len	This field defines the number of octets in the URI string field.
URI	This field contains a UTF-8 string providing a URI for the provided content. Some SCAP results make references to other SCAP result documents by their URI. This field allows a URI to be associated with content so that these references can be resolved. All URIs within a set of results MUST be unique relative to each other for the message to be well-formed.

Language Len	This field defines the number of octets in the Language string field
Language	This field contains a UTF-8 string identifying the SCAP language of the given SCAP result document. This MUST be the XML namespace of the utilized language.
Version Len	This field defines the number of octets in the Version string field.
Version	This field contains a UTF-8 string identifying the version of the language of the given SCAP result document. This is the language version, not the version of SCAP. Trailing 0s (zeroes) in the version number MUST be dropped.
Content Len	This field defines the number of octets in the Content string field.
Content	This field contains the actual SCAP content as a UTF-8 string. The message must be expressed as XML. The content must validate against the appropriate schema(s), although actual validation by either the IMC or IMV is not required.

Table 8 - SCAP Results Message Fields

All IMCs MUST be able to return complete SCAP results in an SCAP Results Message. The exact languages used in these results will vary depending on the languages of the assessment instructions and the version of SCAP supported by the IMC.

4.10 SCAP Summary Results Message

This message is sent from an IMC to an IMV in response to an SCAP Assessment Message that requested results other than full SCAP results. Results can come in many different forms as specified in the SCAP Assessment Message. This message echoes the IMV's result type fields and then includes the assessment results.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Reserved    |  Result Type  |        Result Parameter Len   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Result Parameter (Variable)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Result Len  |          Result (Variable Length)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 13 - SCAP Summary Results Message

Header Field	Description
Reserved	Reserved for future use. This field MUST be set to zero on transmission and ignored upon reception
Result Type	This field indicates the type of the result being returned. Different SCAP languages express assessment results in different ways, and this field allows the nature of the results to be identified. This field is necessary because the result type returned by the IMC might not be the same as the result type requested by the IMV. Available result types are: <table><tr><th>Value</th><th>Meaning</th></tr><tr><td>0</td><td>MUST NOT be used; disallowed in SCAP Summary Results Messages.</td></tr></table>

		1	Absolute result. The assessment passes if every check in the root assessment instruction document evaluates to a value of "true" or "pass", as appropriate for each individual language, regardless of the language in which that root content is expressed. The Result field MUST either hold "0" (fail) or "1" (pass). The Result Param Len field MUST be set to 0 for this Result Type.
		2	XCCDF scoring model. The result for this assessment is a numeric value computed using one of the XCCDF scoring models. The Result field MUST hold a string expression of this numeric value. This type has an additional parameter value that MUST hold the URI of the XCCDF scoring model, as provided in the XCCDF specification, used to calculate the result. Vendor-defined scoring models MUST NOT be used.
		3	XCCDF Rule list. The Result field for this assessment is a comma-separated list of Rule-id/result pairs. For each evaluated XCCDF rule, the Rule's id value is listed, followed by a comma, followed by the abbreviation of the Rule result, using the abbreviations given in the XCCDF specification. Each evaluated Rule MUST be represented by such a pair, and each pair MUST be separated by a comma. Spaces MUST NOT be inserted into this list. The Result Param Len field MUST be set to 0 for this Result Type.
		4	OVAL Definition list. The Result field for this assessment is a comma-separated list of OVAL Definition id/result pairs. For each evaluated OVAL Definition, the definition's id value is listed, followed by a comma, followed by the string value of the OVAL result as represented by the values of OVAL's ResultEnumeration XML type. Each evaluated Definition MUST be represented by such a pair, and each pair MUST be separated by a comma. Spaces MUST NOT be inserted into this list. The Result Param Len field MUST be set to 0 for this Result Type. Note that if XCCDF assessment instructions served as the root of this assessment, it is potentially possible for a single OVAL Definition to be executed multiple times with different variables resulting in different results each time it is executed. The structure of this Result Type cannot differentiate such results. Therefore, in the case where the IMC does not support the IMV's requested Result Type, the IMC MUST NOT use this summary Result Type unless the root of the assessment was an OVAL Definition document, in which case it MAY use this Result Type.
		5	OCIL Questionnaire list. The Result field for this assessment is a comma-separated list of OCIL Questionnaire id/result pairs. For each evaluated OCIL Questionnaire, the questionnaire's id value is listed, followed by a comma, followed by the string value of the OCIL result as represented by the values of OCIL's ResultType XML type. Each evaluated Questionnaire MUST be represented by such a pair, and each pair

<table>
<tr><td></td><td><table><tr><td></td><td>MUST be separated by a comma. Spaces MUST NOT be inserted into this list. The Result Param Len field MUST be set to 0 for this Result Type.</td></tr></table></td></tr>
<tr><td>Result Param Len</td><td>This field defines the number of octets in the Result Param string field.</td></tr>
<tr><td>Result Param</td><td>This field contains a UTF-8 string providing a parameter used to interpret the result of the assessment. The contents of this field depend on the Result Type field.</td></tr>
<tr><td>Result Len</td><td>This field defines the number of octets in the Result string field.</td></tr>
<tr><td>Result</td><td>This field contains a UTF-8 string providing the result of the assessment. The exact contents of this field depend on the Result Type field and the associated parameter, if any. Note that even if the result is numeric, this field is a string expression of the given number.</td></tr>
</table>

Table 9 - SCAP Summary Results Message Fields

Not every IMC will support every type of summary result. However, every IMC MUST support the absolute scoring model. If the IMV requests a summary result type that is not supported by the IMC, then the IMV MAY return a different summary result type.

4.11 SCAP Error Message

This message is sent in response to fatal errors specific to SCAP messages. If the IMC experiences one of the described error conditions when processing an SCAP message from the IMV, it MUST send back at least one SCAP Error Message. The IMC MAY send back multiple SCAP Error Messages within the IF-M response in order provide a more complete diagnosis of the problem. Each SCAP Error Message must be associated with a single error – IMCs MUST NOT bundle multiple errors into a single message. For example, if there are two missing documents in an assessment, the IMC should not create a single SCAP Error Message that lists both missing documents in its Message field. Instead, the IMC should create two SCAP Error Messages - one for each missing document.

An SCAP Error Message should not accompany any SCAP results. An SCAP Error Message is sent instead of SCAP results due to factors that would prevent the reliable creation of results. An SCAP Error Message always terminates the given exchange.

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Reserved    | Error Type    |          Message Len          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Message(varies)                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 14 - SCAP Error Message

<table>
<tr><th>Header Field</th><th>Description</th></tr>
<tr><td>Reserved</td><td>Reserved for future use. This field MUST be set to zero on transmission and ignored upon reception</td></tr>
<tr><td>Error Type</td><td>This field identifies the type of the error. Options include:<table><tr><th>Value</th><th>Meaning</th></tr><tr><td>0</td><td>Other error. This indicates a fatal error other than one of the errors listed below. The message field may contain additional</td></tr></table></td></tr>
</table>

		diagnostic information.
	1	Content missing. This error MUST be sent by an IMC to an IMV to indicate that content required to meet an SCAP Assessment Request Message was not available on the IMC. Note that in cases where there is an unresolvable reference in the SCAP assessment instructions, the IMC would not necessarily return this message, since SCAP content may support alternative references in case there is a failure to resolve a reference. An SCAP Error Message of this type would only be returned if the missing content prohibited the generation of SCAP results. This error MUST be returned if parameters in an SCAP Content Message or SCAP Assessment Instruction Message referred to a document which could not be found - use this error instead of a Parameter error. The Message field MUST contain the URI of the unreachable document.
	2	Content invalid. This error MUST be sent by an IMC to an IMV to indicate that some SCAP assessment instructions were incorrectly formatted. For example, this would be returned if some SCAP assessment instructions failed to validate against the corresponding language's schema. The Message field MUST contain the URI of the incorrectly formatted document.
	3	Content not supported. Not all tools support every language in SCAP. This message MUST be returned if an assessment failed because assessment instructions required for successful completion of an assessment were expressed using a language that the IMC did not support. This failure might be explicit (e.g., requesting a XCCDF-rooted assessment when the IMC did not support XCCDF) or implicit (e.g., as series of references within the SCAP content eventually lead to assessment instructions the IMC is unable to support.) Note that this error would not automatically be returned if the IMC was sent unsupported assessment instructions, because sometimes SCAP assessment instructions describe alternative ways to assess a target. Likewise, sometimes a particular part of an assessment may not be supported, but the rest of the assessment can proceed and the results can still be computed. For example, a tool might not support a particular suite of OVAL tests, but this can be handled within normal OVAL results by having those particular tests return OVAL results of "error" and the rest of the tests could proceed normally. Such a situation would not warrant an SCAP Error Message, since normal SCAP results could be generated. This type of SCAP Error Message should only be returned if the lack of support prevents the generation of SCAP results. (E.g., the root content of the assessment instructions is expressed using XCCDF but the IMC doesn't support XCCDF.) The Message field MUST contain the URI of the document

<table>
<tr><td></td><td><table>
<tr><td></td><td>whose content was not supported.</td></tr>
<tr><td>4</td><td>Parameter error. This error MUST be sent by the IMC to the IMV to indicate that the parameters in the SCAP Content Message or SCAP Assessment Instruction References Message were invalid. For example, if the parameters specified an OVAL External Variable document, but the assessment used an XCCDF document, which generates its own OVAL Variable document, then this error should be returned.
The Message field MUST contain a copy of the SCAP Assessment Message's 1-octet Parameter Type field, 2-octet Parameter Length field, and the Parameter field, all corresponding to the offending parameter.</td></tr>
<tr><td>5</td><td>Timeout. This error MUST be sent by the IMC to the IMV to indicate that the IMC is terminating an open connection because it has been inactive for too long.</td></tr>
</table>
All other Error Type values are reserved for future use and MUST NOT be used in messages.
Note that an Error Type of 0 MUST only be returned if none of the other error types are appropriate.</td></tr>
<tr><td>Message Len</td><td>This field defines the number of octets in the Message field.</td></tr>
<tr><td>Message</td><td>This field contains a UTF-8 string providing additional information regarding the error. The contents of this field depend upon the Error Type field.</td></tr>
</table>

Table 10 - SCAP Error Message Fields

5 Security Considerations

This section looks at security issues surrounding the use of SCAP content in an IF-M exchange. It does not repeat the security considerations of using IF-M itself, as these are addressed in the IF-M specification itself. [7]

5.1 Trust Relationships

In order to understand what security measures must be in place, this section outlines the trust relationships present in the use of SCAP Messages for IF-M.

5.1.1 SCAP-IMC

SCAP-IMCs are trusted by SCAP-IMVs to:

- Accurately perform and report assessments using identified SCAP assessment instructions
- Honor requests regarding the format of the returned SCAP results
- Accurately record and report all SCAP assessment instructions used in the creation of SCAP results
- Correctly implement some version of SCAP and accurately report as to what version(s) of SCAP they supports
- Maintain the integrity of SCAP assessment content within their cache

5.1.2 IMV

SCAP-IMVs are trusted by SCAP-IMCs to:

- Not maliciously change the contents in the IMC's cache, either by sending so much content as to cause performance problems, or by maliciously modifying SCAP assessment instructions so that the IMC fails to perform the expected assessments
- Protect the confidentiality of assessment results, since they may indicate system vulnerabilities

5.1.3 Vendor-proprietary exchanges

This specification acknowledges that SCAP vendors may wish to use their own protocols to manage some aspects of their assessment client's (i.e., the SCAP-IMC's) behavior. SCAP-IMCs and SCAP-IMVs trust vendor proprietary exchanges to:

- Not interfere in an ongoing SCAP Message exchange - vendor proprietary protocols may be used to manage SCAP-IMCs' state, but are not allowed to change its state in the middle of an SCAP Message exchange (see section 4.3.1)

5.2 Security Threats and Countermeasures

Beyond the trusted relationships described in the previous section, the use of SCAP Messages over IF-M faces a number of potential security attacks that could require targeted security countermeasures.

5.2.1 Measurement Theft

Most SCAP results structures include information meant to identify the target of the given assessment. However, this information is just a series of text fields. As such, it is trivial for an adversary who can capture the measurements from one machine to alter those fields and pass those values off as coming from some other machine.

The only real solution is to prevent the theft of these results in the first place. The IMC SHOULD encrypt SCAP results it sends in order to ensure that they are unavailable to the adversary.

5.2.2 Message Fabrication

Malware present on an endpoint could intercept SCAP Messages and return falsified results. This could allow the malware to trick the IMV into believing that an endpoint complied with a given policy when it did not, in fact, do so. Moreover, since SCAP assessment instructions may contain not only what to assess, but the desired values of such assessments, such malware would already possess an "answer key" to the SCAP assessment, allowing it to generate a passing set of assessment results dynamically.

One way to address this attack would be to send SCAP assessment instructions without - or with false - criteria for evaluation, and then evaluate the actual findings of the IMC against real values on the IMV. This method, however, would require the IMC to return full, verbose SCAP results, which is not feasible over connections with a more limited bandwidth, and even then it is not proof against a sophisticated attacker.

Alternately, some other assessment mechanisms, ideally based on evidence that is extremely difficult for an attacker to corrupt, such as values from a TPM, could be used to verify the health of the SCAP-IMC and its supporting software, such as the TNC Client and other software components used in the generation and transmission of results. Currently, SCAP does not support the collection and sending of TPM measurements, so this information would need to be sent using a separate exchange, such as the PTS Protocol [8]. Verifying that the SCAP-IMC was uncorrupted would then allow trust that the complete range of SCAP results the SCAP-IMC generated were correctly generated.

5.2.3 Denial of Service

There are multiple ways an adversary could attempt to prevent an IMC from usefully responding to an IMV's assessment requests. One way would be to maliciously modify the IMC's assessment instruction document cache so that the documents in the cache do not perform the desired assessments. While these changes would be detected by the IMV through the SCAP Capabilities and Inventory Message that accompanies all results, it would prevent the IMV from getting its desired results.

One way to address this might be to associate assessment instructions with the IMV that provided them. While other IMVs might be able to request assessments based on those assessment instructions, the IMC SHOULD only allow a document in its cache to be changed by the entity that originally provided that document. This would prevent third parties from maliciously changing the cache prior to an assessment.

5.2.4 Remote Content as an Attack Vector

SCAP content often contains references, usually taking the form of a URI and an optional record identifier. It is expected that, in most cases, IMCs will treat all URIs in SCAP references as simple identifiers that are associated with some piece of content they have received from an IMV that has been explicitly labeled with that URI. However, this specification allows IMCs to treat the URIs in SCAP references as URLs and resolve SCAP references by actually requesting content from a given location. This could potentially lead to IMCs pulling content from remote repositories that are not under the enterprise's control. The content in these repositories might differ from an IMV's expectations or might actually be malicious, such as containing formatting that exploits buffer overflows or other vulnerabilities in the IMC's software. The former scenario is not a significant security risk since the changed content would quickly be discovered by the IMV, although it could delay assessments as the client must be re-provisioned with new content.

Malicious content is more problematic. Performing XML validation on the content when it is pulled from a remote location is no defense because the XML validation software might contain a vulnerability the content exploits. To address that, IMCs SHOULD be allowed to be configured with filters that identify valid remote sources of SCAP content. By strictly controlling such a list an enterprise can reduce this risk to acceptable levels.

6 References

6.1 Normative References

[1] Trusted Computing Group, *TNC Architecture for Interoperability*, Specification Version 1.0, Revision 3, April 2005.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", Internet Engineering Task Force RFC 2119, March 1997.

[3] NIST, NIST SP 800-126 Rev 2, *The Technical Specification for the Security Assessment instructions Automation Protocol (SCAP): SCAP Version 1.2,* July 2011, available at http://csrc.nist.gov/publications/PubsNISTIRs.html.

[4] ISO, *Data Elements and interchange formats -- Information interchange -- Representation of dates and times*, ISO 8601:2004, March 2008.

6.2 Informative References

[5] Trusted Computing Group, *TNC IF-IMC*, Specification Version 1.2, February 2007.

[6] Trusted Computing Group, *TNC IF-IMV*, Specification Version 1.2, February 2007.

[7] Trusted Computing Group, *TNC IF-M: TLV Binding*, Specification Version 1.0, March 2010.

[8] Trusted Computing Group, *PTS Protocol: Binding to TNC IF-M*, Specification Version 1.0, August 2011.

[9] The MITRE Corp., CVE, http://cve.mitre.org/

[10] The MITRE Corp., OVAL, http://oval.mitre.org/

[11] NIST, XCCDF, http://scap.nist.gov/specifications/xccdf/

[12] The MITRE Corp., CCE, http://cce.mitre.org/

[13] NIST, CPE, http://scap.nist.gov/specifications/cpe/

[14] FiRST, CVSS, http://www.first.org/cvss/

[15] NIST, OCIL, http://scap.nist.gov/specifications/ocil/

[16] NIST, *The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities*, NIST Interagency Report 7502, December 2010.

[17] NIST, ARF, http://scap.nist.gov/specifications/arf/

7 Change Log

This section of the document provides a fairly complete list of things that were changed in each version of the IF-Template spec. It will be removed in the final version.

7.1 Version v0.01r1

- First draft

7.2 Version v0.04

- Initial creation of protocol messages. Only a single "SCAP Message".

7.3 Version v0.05

- Complete revision of protocol messages. Now consists of SCAP Content, SCAP References, SCAP Summary Results, and SCAP Error
- Addressed several bugs noted by Jon Baker

7.4 Version v0.06

- Complete revision of protocol messages.
- Added protocol exchange diagrams
- Revised use cases to remove cases that discussions appear to have shown to be outside of the area of focus that has come out of discussions
- Addressed several issues raised by Clifford Kahn

7.5 Version v0.07

- Added new and revised existing message exchanges
- Clarified that IMC cache management and controls of periodic assessment are important but beyond the scope of this specification
- Changed the specification so that receiving content that duplicates the filename but not the actual file content of something in the cache replaces the cache content rather than raising an error. Removed the corresponding File Integrity Failure error message.
- Added an Exchange ID field to all messages so that all messages in the exchange can be linked to each other by the IMC. This is used to prevent possible race conditions.
- Removed the File Bundle Map field from the SCAP References Message.
- Added a parameter in an SCAP Assessment Message to allow the IMV to specify a subset of OVAL Definitions to use within an OVAL file.
- Added an error message to allow IMCs to terminate exchanges due to timeout.

7.6 Version v0.09

- Many clean-up actions of the text
- Significantly thinned the references to SCAP content, in favor of "SCAP assessment instructions" or "SCAP results" to reduce ambiguity
- Removed the Exchange ID field from all messages since the three exchanges can now occur independently of each other

- Reworked all exchanges to make the three "phases" mentioned in previous versions into separate exchanges. This better supports integration with existing vendor protocols, especially those protocols dealing with content management.
- Added Security Considerations

7.7 Version v0.12

- Address many comments from external reviewers.
- Refactored the terms "file" and "filename" and instead used "document" and "URI" to more strongly disassociate the logical constructs of SCAP content with how they are stored.
- Clarified how URIs associated with documents play into the resolution of SCAP references
- Added the ability of IMVs to influence the type of full SCAP results an IMC returns

7.8 Version v0.13

- Minor clean-up of text

7.9 Version v0.14

- Address additional Dave Waltermire comments

7.10 Version v0.15

- Address comments from reviewers