Security Automation and Continuous Monitoring (SACM) Architecture
draft-ietf-sacm-arch-01

Abstract

This memo defines a Security Automation and Continuous Monitoring (SACM) architecture. This work is built upon [I-D.ietf-mile-xmpp-grid], and is predicated upon information gleaned from SACM Use Cases and Requirements ([RFC7632] and [RFC8248] respectively), and terminology as found in [I-D.ietf-sacm-terminology].

WORKING GROUP: The source for this draft is maintained in GitHub. Suggested changes should be submitted as pull requests at https://github.com/sacmwg/ietf-mandm-sacm-arch/. Instructions are on that page as well.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 26, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of
1. Introduction

The purpose of this draft is to define an architectural solution for a SACM Domain. This draft also defines an implementation of the architecture, built upon [I-D.ietf-mile-xmpp-grid] and [I-D.ietf-sacm-ecp]. These approaches complement each other to more completely meet the spirit of [RFC7632] and requirements found in [RFC8248].
This solution gains the most advantage by supporting a variety of collection mechanisms. In this sense, the solution ideally intends to enable a cooperative ecosystem of tools from disparate sources with minimal operator configuration. The solution described in this document seeks to accommodate these recognitions by first defining a generic abstract architecture, then making that solution somewhat more concrete.

Keep in mind that, at this point, the draft is tracking ongoing work being performed primarily around and during IETF hackathons. The list of hackathon efforts follows:

- [HACK99]: A partial implementation of a vulnerability assessment scenario involving an [I-D.ietf-sacm-ecp] implementation, a [RFC8322] implementation, and a proprietary evaluator to pull the pieces together.

- [HACK100]: Work to combine the vulnerability assessment scenario from [HACK99] with an XMPP-based YANG push model.

- [HACK101]: A fully automated configuration assessment implementation using XMPP as a communication mechanism.

- [HACK102]: An exploration of how we might model assessment, collection, and evaluation abstractly, and then rely on YANG expressions for the attributes of traditional endpoints.

1.1. Open Questions

[NOTE: This section will eventually be removed.]

The following is a list of open questions we still have about the path forward with this exploration:

- Should workflows be documented in this draft or separate drafts?

- Should interfaces be documented in workflow drafts or separate drafts (or even this draft)?

1.2. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119, BCP 14 [RFC2119].
2. Terms and Definitions

This draft defers to [I-D.ietf-sacm-terminology] for terms and definitions.

3. Architectural Overview

The generic approach proposed herein recognizes the need to obtain information from existing state collection mechanisms, and makes every attempt to respect [RFC7632] and [RFC8248]. At the foundation of any architecture are entities, or components, that need to communicate. They communicate by sharing information, where, in a given flow one or more components are consumers of information and one or more components are providers of information.

```
+--------------------+
| Feeds/Repositories |
| of External Data   |
+--------------------+
```

```
*******************************************************************************
|                                 |                                 |
* |                                 |                                 |
* |                                 |                                 |
* |                                 |                                 |
* |                                 |                                 |
* |                                 |                                 |
*******************************************************************************
```

Figure 1: Notional Architecture

As shown in Figure 1, the notional SACM architecture consists of some basic SACM Components using a message transfer system to communicate. While not depicted, the message transfer system is expected to maximally align with the requirements described in [RFC8248], which
means that the message transfer system will support brokered (i.e. point-to-point) and proxied data exchange.

Additionally, component-specific interfaces (i.e. such as A, B, C, D, and E in Figure 1) are expected to be specified logically then bound to one or more specific implementations. This SHOULD be done for each capability related to the given SACM Component.

3.1. SACM Roles

This document suggests a variety of players in a cooperative ecosystem - we call these players SACM Components. SACM Components may be composed of other SACM Components, and each SACM Component plays one, or more, of several roles relevant to the ecosystem. Generally each role is either a consumer of information or a provider of information. The "Components, Capabilities, Interfaces, and Workflows" section provides more details about SACM Components that play these types of roles.

3.2. Exploring An XMPP-based Solution

Figure 2 depicts a slightly more detailed view of the architecture (within the enterprise boundary) - one that fosters the development of a pluggable ecosystem of cooperative tools. Existing collection mechanisms can be brought into this architecture by specifying the interface of the collector and creating the XMPP-Grid Connector binding for that interface.

Additionally, while not directly depicted in Figure 2, this architecture does allow point-to-point interfaces. In fact, [I-D.ietf-mile-xmpp-grid] provides brokering capabilities to facilitate such point-to-point data transfers). Additionally, each of the SACM Components depicted in Figure 2 may be a provider, a consumer, or both, depending on the workflow in context.
[I-D.ietf-mile-xmpp-grid] details a number of XMPP extensions (XEPs) that MUST be utilized to meet the needs of [RFC7632] and [RFC8248]:

- Service Discovery (XEP-0030): Service Discovery allows XMPP entities to discover information about other XMPP entities. Two kinds of information can be discovered: the identity and capabilities of an entity, such as supported features, and items associated with an entity.

- Publish-Subscribe (XEP-0060): The PubSub extension enables entities to create nodes (topics) at a PubSub service and publish information at those nodes. Once published, an event notification is broadcast to all entities that have subscribed to that node.

At this point, [I-D.ietf-mile-xmpp-grid] specifies fewer features than SACM requires, and there are other XMPP extensions (XEPs) we need to consider to meet the needs of [RFC7632] and [RFC8248]. In Figure 2 we therefore use "XMPP-Grid+" to indicate something more than [I-D.ietf-mile-xmpp-grid] alone, even though we are not yet fully confident in the exact set of XMPP-related extensions we will require. The authors propose work to extend (or modify) [I-D.ietf-mile-xmpp-grid] to include additional XEPs - possibly the following:

- Entity Capabilities (XEP-0115): This extension defines the methods for broadcasting and dynamically discovering an entities' capabilities. This information is transported via standard XMPP

Figure 2: XMPP-based Architecture
Example capabilities that could be discovered could include support for posture attribute collection, support for specific types of posture attribute collection such as EPCP, SWIMA, OVAL, or YANG. Other capabilities are still to be determined.

- Ad Hoc Commands (XEP-0050): This extension allows an XMPP entity to advertise and execute application-specific commands. Typically the commands contain data forms (XEP-0004) in order to structure the information exchange. This extension may be usable for simple orchestration (i.e. "do assessment").

- HTTP File Upload (XEP-0363): The HTTP File Upload extension allows for large data sets to be published to a specific path on an HTTP server, and receive a URL from which that file can later be downloaded again. XMPP messages and IQs are meant to be compact, and large data sets, such as collected posture attributes, may exceed a message size threshold. Usage of this XEP allows those larger data sets to be persisted, thus necessitating only the download URL to be passed via XMPP messages.

- Personal Eventing Protocol (XEP-0163): The Personal Eventing Protocol can be thought of as a virtual PubSub service, allowing an XMPP account to publish events only to their roster instead of a generic PubSub topic. This XEP may be useful in the cases when collection requests or queries are only intended for a subset of endpoints and not an entire subscriber set.

- File Repository and Sharing (XEP-0214): This extension defines a method for XMPP entities to designate a set of file available for retrieval by other users of their choosing, and is based on PubSub Collections.

- Easy User Onboarding (XEP-401): The goal of this extension is simplified client registration, and may be useful when adding new endpoints or SACM components to the ecosystem.

- Bidirectional-streams Over Synchronous HTTP (BOSH) (XEP-0124): BOSH emulates the semantics of a long-lived, bidirectional TCP connection between two entities (aka "long polling"). Consider a SACM component that is updated dynamically, i.e. an internal vulnerability definition repository ingesting data from a Feed/Repository of External Data, and a second SACM component such as an Orchestrator. Using BOSH, the Orchestrator can effectively continuously poll the vulnerability definition repository for changes/updates.
PubSub Collection Nodes (XEP-0248): Effectively an extension to XEP-0060 (Publish-Subscribe), PubSub Collections aim to simplify an entities’ subscription to multiple related topics, and establishes a "node graph" relating parent nodes to its descendents. An example "node graph" could be rooted in a "vulnerability definitions" topic, and contain descendent topics for OS family-level vulnerability definitions (i.e. Windows), and further for OS family version-level definitions (i.e. Windows 10 or Windows Server 2016).

PubSub Since (XEP-0312): This extension enables a subscriber to automatically receive PubSub and Personal Eventing Protocol (PEP) notifications since its last logout time. This extension may be useful in intermittent connection scenarios, or when entities disconnect and reconnect to the ecosystem.

PubSub Chaining (XEP-0253): This extension describes the federation of publishing nodes, enabling a publish node of one server to be a subscriber to a publishing node of another server.

3.3. Example Architecture using XMPP-Grid and Endpoint Posture Collection Protocol

Figure 3 depicts a further detailed view of the architecture including the Endpoint Posture Collection Protocol as the collection subsystem, illustrating the idea of a pluggable ecosystem of cooperative tools.
Figure 3: XMPP-based Architecture including EPCP
4. Components, Capabilities, Interfaces, and Workflows

The SACM Architecture consists of a variety of SACM Components, and named components are intended to embody one or more specific capabilities. Interacting with these capabilities will require at least two levels of interface specification. The first is a logical interface specification, and the second is at least one binding to a specific transfer mechanism. An example transfer mechanism is XMPP-Grid+.

The following subsections describe some of the components, capabilities, and interfaces we may expect to see participating in a SACM Domain.

4.1. Components

The following is a list of suggested SACM Component classes and specializations.

- Repository
  - Vulnerability Information Repository
  - Asset Inventory Repository
    - Software Inventory Repository
    - Device Inventory Repository
  - Configuration Policy Repository
  - Configuration State Repository

- Collector
  - Vulnerability State Collector
  - Asset Inventory Collector
    - Software Inventory Collector
    - Device Inventory Collector
  - Configuration State Collector

- Evaluator
  - Vulnerability State Evaluator

Montville & Munyan Expires August 26, 2019
4.2. Capabilities

Repositories will have a need for fairly standard CRUD operations and query by attribute operations. Collector interfaces may enable ad hoc assessment (on-demand processing), state item watch actions (i.e. watch a particular item for particular change), persisting other behaviors (i.e. setting some mandatory reporting period). Evaluators may have their own set of interfaces, and an Assessor would represent both Collector and Evaluation interfaces, and may have additional concerns added to an Assessor Interface.

Not to be overlooked, whatever solution at which we arrive, per [RFC8248], MUST support capability negotiation. While not explicitly treated here, each interface will understand specific serializations, and other component needs to express those serializations to other components.

A capability language is fully explored in mandl-sacm-tool-capability-language (to be submitted).

4.3. Interfaces

Interfaces should be derived directly from identified workflows, several of which are described in this document.
4.4. Workflows

The workflows described in this document should be considered as candidate workflows - informational for the purpose of discovering the necessary components and specifying their interfaces.

4.4.1. IT Asset Management

Information Technology asset management is easier said than done. The [CISCONTROLS] have two controls dealing with IT asset management. Control 1, Inventory and Control of Hardware Assets, states, "Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access." Control 2, Inventory and Control of Software Assets, states, "Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution."

In spirit, this covers all of the processing entities on your network (as opposed to things like network cables, dongles, adapters, etc.), whether physical or virtual.

An IT asset management capability needs to be able to:

- Identify and catalog new assets by executing Target Endpoint Discovery Tasks
- Provide information about its managed assets, including uniquely identifying information (for that enterprise)
- Handle software and/or hardware (including virtual assets)
- Represent cloud hybrid environments

4.4.2. Vulnerability Management

Vulnerability management is a relatively established process. According to the [CISCONTROLS], continuous vulnerability management the act of continuously acquiring, assessing, and taking subsequent action on new information in order to identify and remediate vulnerabilities, therefore minimizing the window of opportunity for attackers.
4.4.2.1. Vulnerability Assessment Workflow Assumptions

A number of assumptions must be stated to clarify the scope of a vulnerability assessment workflow:

- The enterprise has received vulnerability description information, and that the information has already been processed into vulnerability detection data that the enterprise’s security software tools can understand and use.
- The enterprise has a suitable IT Asset Management capability
- The enterprise has a means of extracting relevant information about enterprise endpoints in a form that is compatible with the vulnerability description data (appropriate Collectors for their technologies)
- All information described in this scenario is available in the vulnerability description data and serves as the basis of assessments.
- The enterprise can provide all relevant information about any endpoint needed to perform the described assessment (the appropriate Repositories are available)
- The enterprise has a mechanism for long-term storage of vulnerability description information, vulnerability detection data, and vulnerability assessment results.
- The enterprise has a procedure for reassessment of endpoints at some point after initial assessment

4.4.2.2. Vulnerability Assessment Workflow

When new vulnerability description information is received by the enterprise, affected endpoints are identified and assessed. The vulnerability is said to apply to an endpoint if the endpoint satisfies the conditions expressed in the vulnerability detection data.

A vulnerability assessment (i.e. vulnerability detection) is performed in two steps:

- Endpoint information collected by the endpoint management capabilities is examined by the vulnerability management capabilities through Evaluation Tasks.
If the data possessed by the endpoint management capabilities is insufficient, a Collection Task is triggered and the necessary data is collected from the target endpoint.

Vulnerability detection relies on the examination of different endpoint information depending on the nature of a specific vulnerability. Common endpoint information used to detect a vulnerability includes:

- A specific software version is installed on the endpoint
- File system attributes
- Specific state attributes

In many cases, the endpoint information needed to determine an endpoint’s vulnerability status will have been previously collected by the endpoint management capabilities and available in a Repository. However, in other cases, the necessary endpoint information will not be readily available in a Repository and a Collection Task will be triggered to collect it from the target endpoint. Of course, some implementations of endpoint management capabilities may prefer to enable operators to perform this collection under certain circumstances, even when sufficient information can be provided by the endpoint management capabilities (e.g. there may be freshness requirements for information).

The collection of additional endpoint information for the purpose of vulnerability assessment does not necessarily need to be a pull by the vulnerability assessment capabilities. Over time, some new pieces of information that are needed during common types of assessments might be identified. Endpoint management capabilities can be reconfigured to have this information delivered automatically. This avoids the need to trigger additional Collection Tasks to gather this information during assessments, streamlining the assessment process. Likewise, it might be observed that certain information delivered by endpoint management capabilities is rarely used. In this case, it might be useful to re-configure the endpoint management capabilities to no longer collect this information to reduce network and processing overhead. Instead, a new Collection Task can be triggered to gather this data on the rare occasions when it is needed.

### 4.4.3. Configuration Management

Configuration management involves configuration assessment, which requires state assessment (TODO: Tie to SACM use cases). The [CISCONTROLS] specify two high-level controls concerning
configuration management (Control 5 for non-network devices and Control 11 for network devices). As an aside, these controls are listed separately because many enterprises have different organizations for managing network infrastructure and workload endpoints. Merging the two controls results in a requirement to: "Establish, implement, and actively manage (track, report on, correct) the security configuration of (endpoints) using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings."

Typically, an enterprise will use configuration guidance from a reputable source, and from time to time they may tailor the guidance from that source prior to adopting it as part of their enterprise standard. The enterprise standard is then provided to the appropriate configuration assessment tools and they assess endpoints and/or appropriate endpoint information. A preferred flow follows:

- Reputable source publishes new or updated configuration guidance
- Enterprise configuration assessment capability retrieves configuration guidance from reputable source
- Optional: Configuration guidance is tailored for enterprise-specific needs
- Configuration assessment tool queries asset inventory repository to retrieve a list of affected endpoints
- Configuration assessment tool queries configuration state repository to evaluate compliance
- If information is stale or unavailable, configuration assessment tool triggers an ad hoc assessment

The SACM architecture needs to support varying deployment models to accommodate the current state of the industry, but should strongly encourage event-driven approaches to monitoring configuration.

5. Privacy Considerations
   TODO

6. Security Considerations
   TODO
7. IANA Considerations

IANA tables can probably be used to make life a little easier. We would like a place to enumerate:

- Capability/operation semantics
- SACM Component implementation identifiers
- SACM Component versions
- Associations of SACM Components (and versions) to specific Capabilities

8. References

8.1. Normative References

[I-D.ietf-mile-xmpp-grid]

[I-D.ietf-sacm-ecp]


8.2. Informative References

[CISCONTROLS]

Montville & Munyan Expires August 26, 2019 [Page 16]
[draft-birkholz-sacm-yang-content]  


[I-D.ietf-sacm-terminology]  

[NIST800126]  

[NISTIR7694]  

Appendix A. Mapping to RFC8248

This section provides a mapping of XMPP and XMPP Extensions to the relevant requirements from [RFC8248]. In the table below, the ID and Name columns provide the ID and Name of the requirement directly out of [RFC8248]. The Supported By column may contain one of several values:

- N/A: The requirement is not applicable to this architectural exploration
- Architecture: This architecture (possibly assuming some components) should meet the requirement
- XMPP: The set of XMPP Core specifications and the collection of applicable extensions, deployment, and operational considerations.
- XMPP-Core: The requirement is satisfied by a core XMPP feature
- XEP-nnnn: The requirement is satisfied by a numbered XMPP extension (see [XMPPEXT])
- Operational: The requirement is an operational concern or can be addressed by an operational deployment
- Implementation: The requirement is an implementation concern

If there is no entry in the Supported By column, then there is a gap that must be filled.

+--------------------------------+--------------------------+
| Montville & Munyan | Expires August 26, 2019 |
+--------------------------------+--------------------------+
<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Supported By</th>
</tr>
</thead>
<tbody>
<tr>
<td>G-001</td>
<td>Solution Extensibility</td>
<td>XMPP-Core</td>
</tr>
<tr>
<td>G-002</td>
<td>Interoperability</td>
<td>XMPP</td>
</tr>
<tr>
<td>G-003</td>
<td>Scalability</td>
<td>XMPP</td>
</tr>
<tr>
<td>G-004</td>
<td>Versatility</td>
<td>XMPP-Core</td>
</tr>
<tr>
<td>G-005</td>
<td>Information Extensibility</td>
<td>XMPP-Core</td>
</tr>
<tr>
<td>G-006</td>
<td>Data Protection</td>
<td>Operational</td>
</tr>
<tr>
<td>G-007</td>
<td>Data Partitioning</td>
<td>Operational</td>
</tr>
<tr>
<td>G-008</td>
<td>Versioning and Backward Compatibility</td>
<td>XEP-0115/0030</td>
</tr>
<tr>
<td>G-009</td>
<td>Information Discovery</td>
<td>XEP-0030</td>
</tr>
<tr>
<td>G-010</td>
<td>Target Endpoint Discovery</td>
<td>XMPP-Core</td>
</tr>
<tr>
<td>G-011</td>
<td>Push and Pull Access</td>
<td>XEP-0060/0312</td>
</tr>
<tr>
<td>G-012</td>
<td>SACM Component Interface</td>
<td>N/A</td>
</tr>
<tr>
<td>G-013</td>
<td>Endpoint Location and Network Topology</td>
<td></td>
</tr>
<tr>
<td>G-014</td>
<td>Target Endpoint Identity</td>
<td>XMPP-Core</td>
</tr>
<tr>
<td>G-015</td>
<td>Data Access Control</td>
<td></td>
</tr>
<tr>
<td>ARCH-001</td>
<td>Component Functions</td>
<td>XMPP</td>
</tr>
<tr>
<td>ARCH-002</td>
<td>Scalability</td>
<td>XMPP-Core</td>
</tr>
<tr>
<td>ARCH-003</td>
<td>Flexibility</td>
<td>XMPP-Core</td>
</tr>
<tr>
<td>ARCH-004</td>
<td>Separation of Data and Management Functions</td>
<td></td>
</tr>
<tr>
<td>ARCH-005</td>
<td>Topology Flexibility</td>
<td>XMPP-Core</td>
</tr>
<tr>
<td>ARCH-006</td>
<td>Capability Negotiation</td>
<td>XEP-0115/0030</td>
</tr>
<tr>
<td>ARCH-007</td>
<td>Role-Based Authorization</td>
<td>XMPP-Core</td>
</tr>
<tr>
<td>ARCH-008</td>
<td>Context-Based Authorization</td>
<td></td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td>Category</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ARCH-009</td>
<td>Time Synchronization</td>
<td>Operational</td>
</tr>
<tr>
<td>IM-001</td>
<td>Extensible Attribute Vocabulary</td>
<td>N/A</td>
</tr>
<tr>
<td>IM-002</td>
<td>Posture Data Publication</td>
<td>N/A</td>
</tr>
<tr>
<td>IM-003</td>
<td>Data Model Negotiation</td>
<td>N/A</td>
</tr>
<tr>
<td>IM-004</td>
<td>Data Model Identification</td>
<td>N/A</td>
</tr>
<tr>
<td>IM-005</td>
<td>Data Lifetime Management</td>
<td>N/A</td>
</tr>
<tr>
<td>IM-006</td>
<td>Singularity and Modularity</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-001</td>
<td>Element Association</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-002</td>
<td>Data Model Structure</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-003</td>
<td>Search Flexibility</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-004</td>
<td>Full vs. Partial Updates</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-005</td>
<td>Loose Coupling</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-006</td>
<td>Data Cardinality</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-007</td>
<td>Data Model Negotiation</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-008</td>
<td>Data Origin</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-009</td>
<td>Origination Time</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-010</td>
<td>Data Generation</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-011</td>
<td>Data Source</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-012</td>
<td>Data Updates</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-013</td>
<td>Multiple Collectors</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-014</td>
<td>Attribute Extensibility</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-015</td>
<td>Solicited vs. Unsolicited Updates</td>
<td>N/A</td>
</tr>
<tr>
<td>DM-016</td>
<td>Transfer Agnostic</td>
<td>N/A</td>
</tr>
<tr>
<td>OP-001</td>
<td>Time Synchronization</td>
<td></td>
</tr>
</tbody>
</table>
### Appendix B. Example Components

#### B.1. Policy Services

Consider a policy server conforming to [RFC8322]. [RFC8322] describes a RESTful way based on the ATOM Publishing Protocol ([RFC5023]) to find specific data collections. While this represents a specific binding (i.e. RESTful API based on [RFC5023]), there is a more abstract way to look at ROLIE.

ROLIE provides notional workspaces and collections, and provides the concept of information categories and links. Strictly speaking, these are logical concepts independent of the RESTful binding ROLIE specifies. In other words, ROLIE binds a logical interface (i.e. GET workspace, GET collection, SET entry, and so on) to a specific mechanism (namely an ATOM Publication Protocol extension).
It is not inconceivable to believe there could be a different interface mechanism, or a connector, providing these same operations using XMPP-Grid as the transfer mechanism.

Even if a [RFC8322] server were external to an organization, there would be a need for a policy source inside the organization as well, and it may be preferred for such a policy source to be connected directly to the ecosystem’s communication infrastructure.

B.2. Software Inventory

The SACM working group has accepted work on the Endpoint Posture Collection Profile [I-D.ietf-sacm-ecp], which describes a collection architecture and may be viewed as a collector coupled with a collection-specific repository.

```
+--------+      +-----------+ |        | +-----------+ |
|        |      | +-----------+ |        | +-----------+ |
|        |<---->| | Posture   | |        | | Posture   | |
|        | pub/ | | Validator | |        | | Collector | |
|        | sub  | +-----------+ |        | +-----------+ |
+--------+      |      |        |        |      |        |
|      |        |        |      |        |      |        |
|      |<-----> |        |<-----| | Posture   | | report | | Posture   | |
|      |request/|        | store| +-----------+ |------->| +-----------+ |
|      |respond |        |      |               |        |               |
+------+        +--------+      +---------------+        +---------------+
```

Figure 4: EPCP Collection Architecture

In Figure 4, any of the communications between the Posture Manager and EPCP components to its left could be performed directly or indirectly using a given message transfer mechanism. For example, the pub/sub interface between the Orchestrator and the Posture Manager could be using a proprietary method or using [I-D.ietf-mile-xmpp-grid] or some other pub/sub mechanism. Similarly, the store connection from the Posture Manager to the Repository could be performed internally to a given implementation, via a RESTful API invocation over HTTPS, or even over a pub/sub mechanism.
Our assertion is that the Evaluator, Repository, Orchestrator, and Posture Manager all have the potential to represent SACM Components with specific capability interfaces that can be logically specified, then bound to one or more specific transfer mechanisms (i.e. RESTful API, [RFC8322], [I-D.ietf-mile-xmpp-grid], and so on).

B.3. Datastream Collection

[NIST800126], also known as SCAP 1.3, provides the technical specifications for a "datastream collection". The specification describes the "datastream collection" as being "composed of SCAP data streams and SCAP source components". A "datastream" provides an encapsulation of the SCAP source components required to, for example, perform configuration assessment on a given endpoint. These source components include XCCDF checklists, OVAL Definitions, and CPE Dictionary information. A single "datastream collection" may encapsulate multiple "datastreams", and reference any number of SCAP components. Datastream collections were intended to provide an envelope enabling transfer of SCAP data more easily.

The [NIST800126] specification also defines the "SCAP result data stream" as being conformant to the Asset Reporting Format specification, defined in [NISTIR7694]. The Asset Reporting Format provides an encapsulation of the SCAP source components, Asset Information, and SCAP result components, such as system characteristics and state evaluation results.

What [NIST800126] did not do is specify the interface for finding or acquiring source datastream information, nor an interface for publishing result information. Discovering the actual resources for this information could be done via ROLIE, as described in the Policy Services section above, but other repositories of SCAP data exist as well.

B.4. Network Configuration Collection

[draft-birkholz-sacm-yang-content] illustrates a SACM Component incorporating a YANG Push client function and an XMPP-grid publisher function. [draft-birkholz-sacm-yang-content] further states "the output of the YANG Push client function is encapsulated in a SACM Content Element envelope, which is again encapsulated in a SACM statement envelope" which are published, essentially, via an XMPP-Grid Connector for SACM Components also part of the XMPP-Grid.

This is a specific example of an existing collection mechanism being adapted to the XMPP-Grid message transfer system.
Authors’ Addresses

Adam W. Montville
Center for Internet Security
31 Tech Valley Drive
East Greenbush, NY 12061
USA

Email: adam.w.montville@gmail.com

Bill Munyan
Center for Internet Security
31 Tech Valley Drive
East Greenbush, NY 12061
USA

Email: bill.munyan.ietf@gmail.com
Concise Software Identification Tags
draft-ietf-sacm-coswid-10

Abstract

This document defines a concise representation of ISO/IEC 19770-2:2015 Software Identification (SWID) tags that are interoperable with the XML schema definition of ISO/IEC 19770-2:2015. Next to the inherent capability of SWID tags to express arbitrary context information, Concise SWID (CoSWID) tags support the definition of additional semantics via well-defined data definitions incorporated by extension points.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 26, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents
Table of Contents

1. Introduction ............................................. 3
   1.1. The SWID and CoSWID Tag Lifecycle ..................... 4
   1.2. Concise SWID Format ..................................... 6
   1.3. Requirements Notation .................................... 7

2. Concise SWID Data Definition ............................... 7
   2.1. Concise SWID Extensions ................................. 8
   2.2. The concise-swid-tag Group ............................... 9
   2.3. concise-swid-tag Co-constraints ......................... 13
   2.4. The global-attributes Group ............................. 14
   2.5. The entity-entry Group .................................. 15
   2.6. The link-entry Map ...................................... 17
   2.7. The software-meta-entry Map ............................. 21
   2.8. The Resource Collection Definition ..................... 24
      2.8.1. The hash-entry Array ................................ 24
      2.8.2. The resource-collection Group ....................... 24
      2.8.3. The payload-entry Group .............................. 27
      2.8.4. The evidence-entry Group ............................ 28
   2.9. Full CDDL Definition .................................... 28

3. Determining the Type of CoSWID ............................. 34

4. CoSWID Indexed Label Values ................................. 34
   4.1. Version Scheme .......................................... 34
   4.2. Entity Role Values ....................................... 35
   4.3. Link Ownership Values .................................... 36
   4.4. Link Rel Values .......................................... 37
   4.5. Link Use Values .......................................... 39

5. IANA Considerations ......................................... 39
   5.1. CoSWID Items Registry .................................... 39
   5.2. SWID/CoSWID Value Registries ............................ 42
      5.2.1. SWID/CoSWID Version Scheme Value Registry .......... 43
      5.2.2. SWID/CoSWID Entity Role Value Registry .............. 44
      5.2.3. SWID/CoSWID Link Ownership Value Registry ........... 45
      5.2.4. SWID/CoSWID Link Relationship Value Registry ......... 46
      5.2.5. SWID/CoSWID Link Use Value Registry ................. 47
   5.3. swid+cbor Media Type Registration ...................... 48
   5.4. CoAP Content-Format Registration ....................... 49
   5.5. CBOR Tag Registration .................................... 50

6. Security Considerations .................................... 50

7. Acknowledgments ............................................ 52
1. Introduction

SWID tags have several use-applications including but not limited to:

- Software Inventory Management, a part of a Software Asset Management [SAM] process, which requires an accurate list of discernible deployed software components.

- Vulnerability Assessment, which requires a semantic link between standardized vulnerability descriptions and software components installed on IT-assets [X.1520].

- Remote Attestation, which requires a link between reference integrity measurements (RIM) and security logs of measured software components [I-D.birkholz-rats-tuda].

SWID tags, as defined in ISO-19770-2:2015 [SWID], provide a standardized XML-based record format that identifies and describes a specific release of a software component. Different software components, and even different releases of a particular software component, each have a different SWID tag record associated with them. SWID tags are meant to be flexible and able to express a broad set of metadata about a software component.

While there are very few required fields in SWID tags, there are many optional fields that support different use scenarios. A SWID tag consisting of only required fields might be a few hundred bytes in size; however, a tag containing many of the optional fields can be many orders of magnitude larger. Thus, real-world instances of SWID tags can be fairly large, and the communication of SWID tags in use-applications, such as those described earlier, can cause a large amount of data to be transported. This can be larger than acceptable for constrained devices and networks. Concise SWID (CoSWID) tags significantly reduce the amount of data transported as compared to a typical SWID tag. This reduction is enabled through the use of CBOR, which maps the human-readable labels of SWID data items to more concise integer labels (indices). The use of CBOR to express SWID information in CoSWID tags allows both CoSWID and SWID tags to be part of an enterprise security solution for a wider range of endpoints and environments.
1.1. The SWID and CoSWID Tag Lifecycle

In addition to defining the format of a SWID tag record, ISO/IEC 19770-2:2015 defines requirements concerning the SWID tag lifecycle. Specifically, when a software component is installed on an endpoint, that software component’s SWID tag is also installed. Likewise, when the software component is uninstalled or replaced, the SWID tag is deleted or replaced, as appropriate. As a result, ISO/IEC 19770-2:2015 describes a system wherein there is a correspondence between the set of installed software components on an endpoint, and the presence of the corresponding SWID tags for these components on that endpoint. CoSWIDs share the same lifecycle requirements as a SWID tag.

The SWID specification and supporting guidance provided in NIST Internal Report (NISTIR) 8060: Guidelines for the Creation of Interoperable SWID Tags [SWID-GUIDANCE] defines four types of SWID tags: primary, patch, corpus, and supplemental.

1. Primary Tag - A SWID or CoSWID tag that identifies and describes a software component is installed on a computing device. A primary tag is intended to be installed on an endpoint along with the corresponding software component.

2. Patch Tag - A SWID or CoSWID tag that identifies and describes an installed patch which has made incremental changes to a software component installed on an endpoint. A patch tag is intended to be installed on an endpoint along with the corresponding software component patch.

3. Corpus Tag - A SWID or CoSWID tag that identifies and describes an installable software component in its pre-installation state. A corpus tag can be used to represent metadata about an installation package or installer for a software component, a software update, or a patch.

4. Supplemental Tag - A SWID or CoSWID tag that allows additional information to be associated with a referenced SWID tag. This helps to ensure that SWID Primary and Patch Tags provided by a software provider are not modified by software management tools, while allowing these tools to provide their own software metadata.

The type of a tag is determined by specific data elements, which is discussed in Section 3.

Corpus, primary, and patch tags have similar functions in that they describe the existence and/or presence of different types of
software (e.g., software installers, software installations, software patches), and, potentially, different states of software components. In contrast, supplemental tags furnish additional information not contained in corpus, primary, or patch tags. All four tag types come into play at various points in the software lifecycle, and support software management processes that depend on the ability to accurately determine where each software component is in its lifecycle.

Figure 1: Use of Tag Types in the Software Lifecycle

Figure 1 illustrates the steps in the software lifecycle and the relationships among those lifecycle events supported by the four types of SWID and CoSWID tags, as follows:

* **Software Deployment.** Before the software component is installed (i.e., pre-installation), and while the product is being deployed, a corpus tag provides information about the installation files and distribution media (e.g., CD/DVD, distribution package).

* **Software Installation.** A primary tag will be installed with the software component (or subsequently created) to uniquely identify and describe the software component. Supplemental tags are created to augment primary tags with additional site-specific or extended information. While not illustrated in the figure, patch tags can also be installed during software installation to provide information about software fixes deployed along with the base software installation.

* **Software Patching.** When a new patch is applied to the software component, a new patch tag is provided, supplying details about the patch and its dependencies. While not illustrated in the
figure, a corpus tag can also provide information about the patch installer, and patching dependencies that need to be installed before the patch.

* Software Upgrading. As a software component is upgraded to a new version, new primary and supplemental tags replace existing tags, enabling timely and accurate tracking of updates to software inventory. While not illustrated in the figure, a corpus tag can also provide information about the upgrade installer, and dependencies that need to be installed before the upgrade.

* Software Removal. Upon removal of the software component, relevant SWID tags are removed. This removal event can trigger timely updates to software inventory reflecting the removal of the product and any associated patch or supplemental tags.

Note: While not fully illustrated in the figure, supplemental tags can be associated with any corpus, primary, or patch tag to provide additional metadata about an installer, installed software, or installed patch respectively.

Understanding the use of CoSWIDs in the software lifecycle provides a basis for understanding the information provided in a CoSWID and the associated semantics of this information. Each of the different SWID and CoSWID tag types provide different sets of information. For example, a "corpus tag" is used to describe a software component’s installation image on an installation media, while a "patch tag" is meant to describe a patch that modifies some other software component.

1.2. Concise SWID Format

This document defines the CoSWID tag format, a more concise representation of SWID information in the Concise Binary Object Representation (CBOR) [RFC7049]. The structure of a CoSWID is described via the Concise Data Definition Language (CDDL) [RFC8610]. The resulting CoSWID data definition is aligned to the information able to be expressed with the XML schema definition of ISO-19770-2:2015 [SWID]. This alignment allows both SWID and CoSWID tags to represent a common set of SWID information and to support all SWID tag use cases. To achieve this end, the CDDL representation includes every SWID tag field and attribute.

The vocabulary, i.e., the CDDL names of the types and members used in the CoSWID data definition, are mapped to more concise labels represented as small integer values. The names used in the CDDL data definition and the mapping to the CBOR representation using integer
labels is based on the vocabulary of the XML attribute and element names defined in ISO/IEC 19770-2:2015.

1.3. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Concise SWID Data Definition

The following is a CDDL representation for a CoSWID tag. The CamelCase notation used in the XML schema definition is changed to a hyphen-separated notation KebabCase (e.g., ResourceCollection is named resource-collection) in the CoSWID data definition. In essence, KebabCase "looks-like-this". This deviation from the original notation used in the XML representation reduces ambiguity when referencing certain attributes in corresponding textual descriptions. An attribute referred to by its name in CamelCase notation explicitly relates to XML SWID tags; an attribute referred to by its name in KebabCase notation explicitly relates to CoSWID tags. This approach simplifies the composition of further work that reference both XML SWID and CoSWID documents.

Human-readable labels of members in CDDL map data definitions are mapped to integer indices via a block of rules at the bottom of the definition. The 57 character strings of the SWID vocabulary are replaced which would have to be stored or transported in full if using the original vocabulary.

In CBOR, an array is encoded using bytes that identify the array, and the array’s length or stop point (see [RFC7049]). To make items that support 1 or more values, the following CDDL notion is used.

```cddl
_name_ = (_label_: _data_ / [ 2* _data_ ])
```

The CDDL rule above allows for a more efficient CBOR encoding of the data when a single value is used. This is accomplished by avoiding the need to first encode the array. Conversely, hen two or more values are encoded, the bytes identifying the array are used. This modeling pattern is used frequently in the CoSWID CDDL data definition to allow for more efficient encoding of single values.

The following subsections describe the different parts of the CoSWID model.
2.1. Concise SWID Extensions

The corresponding CoSWID data definition includes two kinds of augmentation.

- The explicit definition of types for attributes that are typically stored in the "any attribute" of an ISO-19770-2:2015 in XML representation. These are covered in Section 2.4.

- The inclusion of extension points in the CoSWID data definition using CDDL sockets (see [RFC8610] section 3.9). The use of CDDL sockets allow for well-formed extensions to be defined in supplementary CDDL descriptions that support additional uses of CoSWID tags that go beyond the original scope of ISO-19770-2:2015 tags. This extension mechanism can also be used to update the CoSWID format as revisions to ISO-19770-2 are published.

The following CDDL sockets (extension points) are defined in this document, which allow the addition of new information structures to their respective CDDL groups.

<table>
<thead>
<tr>
<th>Map Name</th>
<th>CDDL Socket</th>
<th>Defined in</th>
</tr>
</thead>
<tbody>
<tr>
<td>concise-swid-tag</td>
<td>$$coswid-extension</td>
<td>Section 2.2</td>
</tr>
<tr>
<td>entity-entry</td>
<td>$$entity-extension</td>
<td>Section 2.5</td>
</tr>
<tr>
<td>link-entry</td>
<td>$$link-extension</td>
<td>Section 2.6</td>
</tr>
<tr>
<td>software-meta-entry</td>
<td>$$meta-extension</td>
<td>Section 2.7</td>
</tr>
<tr>
<td>file-entry</td>
<td>$$file-extension</td>
<td>Section 2.8.2</td>
</tr>
<tr>
<td>directory-entry</td>
<td>$$directory-extension</td>
<td>Section 2.8.2</td>
</tr>
<tr>
<td>process-entry</td>
<td>$$process-extension</td>
<td>Section 2.8.2</td>
</tr>
<tr>
<td>resource-entry</td>
<td>$$resource-extension</td>
<td>Section 2.8.2</td>
</tr>
<tr>
<td>payload-entry</td>
<td>$$payload-extension</td>
<td>Section 2.8.3</td>
</tr>
<tr>
<td>evidence-entry</td>
<td>$$evidence-extension</td>
<td>Section 2.8.4</td>
</tr>
</tbody>
</table>

The CoSWID Items Registry defined in Section 5.1 provides a registration mechanism allowing new items, and their associated index values, to be added to the CoSWID model through the use of the CDDL.
sockets described above. This registration mechanism provides for
well-known index values for data items in CoSWID extensions, allowing
these index values to be recognized by implementations supporting a
given extension.

The following CDDL sockets defined in this document allow for adding
new values to corresponding type-choices (i.e. to represent
enumerations) via custom CDDL data definitions.

<table>
<thead>
<tr>
<th>Enumeration Name</th>
<th>CDDL Socket</th>
<th>Defined in</th>
</tr>
</thead>
<tbody>
<tr>
<td>version-scheme</td>
<td>$version-scheme</td>
<td>Section 4.1</td>
</tr>
<tr>
<td>role</td>
<td>$role</td>
<td>Section 4.2</td>
</tr>
<tr>
<td>ownership</td>
<td>$ownership</td>
<td>Section 4.3</td>
</tr>
<tr>
<td>rel</td>
<td>$rel</td>
<td>Section 4.4</td>
</tr>
<tr>
<td>use</td>
<td>$use</td>
<td>Section 4.5</td>
</tr>
</tbody>
</table>

A number of SWID/CoSWID value registries are also defined in
Section 5.2 that allow new valid values to be registered with IANA
for the enumerations above. This registration mechanism supports the
definition of new well-known index values and names for new
enumeration values used by SWID and CoSWID. This registration
mechanism allows new standardized enumerated values to be shared
between both specifications (and implementations) over time.

2.2. The concise-swid-tag Group

The CDDL data definition for the root concise-swid-tag map is as
follows and this rule and its constraints MUST be followed when
creating or validating a CoSWID tag:
concise-swid-tag = {
  global-attributes,
  tag-id => text,
  tag-version => integer,
  ? corpus => bool,
  ? patch => bool,
  ? supplemental => bool,
  software-name => text,
  ? software-version => text,
  ? version-scheme => $version-scheme,
  ? media => text,
  ? software-meta => software-meta-entry / [ 2* software-meta-entry ],
  entity => entity-entry / [ 2* entity-entry ],
  ? link => link-entry / [ 2* link-entry ],
  ? (( payload => payload-entry ) // ( evidence => evidence-entry )),
  * $$coswid-extension
}

tag-id = 0
software-name = 1
entity = 2
evidence = 3
link = 4
software-meta = 5
payload = 6
corpus = 8
patch = 9
media = 10
supplemental = 11
tag-version = 12
software-version = 13
version-scheme = 14

$version-scheme /= multipartnumeric
$version-scheme /= multipartnumeric-suffix
$version-scheme /= alphanumeric
$version-scheme /= decimal
$version-scheme /= semver
$version-scheme /= uint / text
multipartnumeric = 1
multipartnumeric-suffix = 2
alphanumeric = 3
decimal = 4
semver = 16384

The following describes each member of the concise-swid-tag root map.
- global-attributes: A list of items including an optional language definition to support the processing of text-string values and an unbounded set of any-attribute items. Described in Section 2.4.

- tag-id (index 0): A textual identifier uniquely referencing a (composite) software component. The tag identifier MUST be globally unique. There are no strict guidelines on how this identifier is structured, but examples include a 16 byte GUID (e.g. class 4 UUID) [RFC4122], or a text string appended to a DNS domain name to ensure uniqueness across organizations.

- tag-version (index 12): An integer value that indicate the specific release revision of the tag. Typically, the initial value of this field is set to 0, and the value is monotonically increased for subsequent tags produced for the same software component release. This value allows a CoSWID tag producer to correct an incorrect tag previously released, without indicating a change to the underlying software component the tag represents. For example, the tag version would be changed to add new metadata, to correct a broken link, to add a missing payload entry, etc. When producing a revised tag, the new tag-version value MUST be greater than the old tag-version value.

- corpus (index 8): A boolean value that indicates if the tag identifies and describes an installable software component in its pre-installation state. Installable software includes a installation package or installer for a software component, a software update, or a patch. If the CoSWID tag represents installable software, the corpus item MUST be set to "true". If not provided the default value MUST be considered "false".

- patch (index 9): A boolean value that indicates if the tag identifies and describes an installed patch which has made incremental changes to a software component installed on a computing device. Typically, an installed patch has made a set of file modifications to pre-installed software, and does not alter the version number or the descriptive metadata of an installed software component. If a CoSWID tag is for a patch, the patch item MUST be set to "true". If not provided the default value MUST be considered "false".

- supplemental (index 11): A boolean value that indicates if the tag is providing additional information to be associated with another referenced SWID or CoSWID tag. Tags using this item help to ensure that primary and patch tags provided by a software provider are not modified by software management tools, while allowing these tools to provide their own software metadata for a software component. If a CoSWID tag is a supplemental tag, the
supplemental item MUST be set to "true". If not provided the default value MUST be considered "false".

- software-name (index 1): This textual item provides the software component’s name. This name is likely the same name that would appear in a package management tool.

- software-version (index 13): A textual value representing the specific release or development version of the software component.

- version-scheme (index 14): An 8-bit integer or textual value representing the versioning scheme used for the software-version item. If an integer value is used it MUST be a value from the SWID/CoSWID Version Scheme Value Registry (see section Section 5.2.1 or a value in the private use range: 32768-65535.

An initial set of pre-defined version-scheme index and text values are defined in Section 4.1 that are based on the version-scheme values defined in [SWID]. These pre-defined version-scheme values are registered with IANA in the "SWID/CoSWID Version Scheme Value" registry Section 5.2.1, and MAY be expanded in the future.

The value of an ownership item MUST be one of the following:

* The index (preferred) or string value of a role from the IANA in the "SWID/CoSWID Version Scheme Value" registry.

* An index value in the range 32768 through 65535, to indicate that a private use index value is used.

* A string value prefixed with "x_", to indicate that a private use string value is used.

- media (index 10): This text value is a hint to the tag consumer to understand what this tag applies to. This item represents a query as defined by the W3C Media Queries Recommendation (see [W3C.REC-css3-mediaqueries-20120619]).

- software-meta (index 5): An open-ended map of key/value data pairs. A number of predefined keys can be used within this item providing for common usage and semantics across the industry. Use of this map allows any additional attribute to be included in the tag. It is expected that industry groups will use a common set of attribute names to allow for interoperability within their communities. Described in Section 2.7.

- entity (index 2): Provides information about one or more organizations responsible for producing the CoSWID tag, and
producing or releasing the software component referenced by this CoSWID tag. Described in Section 2.5.

- **link (index 4):** Provides a means to establish relationship arcs between the tag and another items. A given link can be used to establish the relationship between tags or to reference another resource that is related to the CoSWID tag, e.g. vulnerability database association, ROLIE feed [RFC8322], MUD resource [RFC8520], software download location, etc. This is modeled after the HTML "link" element. Described in Section 2.6.

- **payload (index 6):** This item represents the software artifacts that compose the target software. For example, the files included with an installer for a corpus tag or installed on an endpoint when the software component is installed for a primary or patch tag. The artifacts listed in a payload may be a superset of the software artifacts that are actually installed. Based on user selections at install time, an installation might not include every artifact that could be created or executed on the endpoint when the software component is installed or run. Described in Section 2.8.3.

- **evidence-entry (index 3):** This item records the results of a software discovery process used to identify untagged software on an endpoint. This item provides a means to represent indicators for why software is believed to be installed on the endpoint. In such a case, a CoSWID tag is created when the endpoint is scanned by the tool performing the scan. Described in Section 2.8.4.

- **$coswid-extension:** This CDDL socket is used to add new information structures to the concise-swid-tag root map. See Section 2.1.

### 2.3. concise-swid-tag Co-constraints

The following co-constraints apply to the information provided by in the concise-swid-tag group.

- The patch and supplemental items MUST NOT both be set to "true".

- If the patch item is set to "true", the tag SHOULD contain at least one link item with the rel(ation) item value of "patches" and an href item specifying an association with the software that was patched.

- If the supplemental item is set to "true", the tag SHOULD contain at least one link item with the rel(ation) item value of...
"supplements" and an href item specifying an association with the software that is supplemented.

- If all of the corpus, patch, and supplemental items are "false", or if the corpus item is set to "true", then a software-version item MUST be included with a value set to the version of the software component. This ensures that primary and corpus tags have an identifiable software version.

2.4. The global-attributes Group

The global-attributes group provides a list of items including an optional language definition to support the processing of text-string values and an unbounded set of any-attribute items allowing for additional items to be provided as a general point of extension in the model.

The CDDL for the global-attributes follows:

```
global-attributes = ( ? lang, * any-attribute, )


label = text / int
```

The following describes each child item of this group.

- lang (index 15): A textual language tag that conforms with IANA "Language Subtag Registry" [RFC5646]. The context of the specified language applies to all sibling and descendant textual values, unless a descendant object has defined a different language tag. Thus, a new context is established when a descendant object redefines a new language tag. All textual values within a given context MUST be considered expressed in the specified language.

- any-attribute: This sub-group provides a means to include arbitrary information via label ("key") value pairs. Labels can be either a single integer or text string. Values can be either a single integer or text string, or an array of integers or text strings.
2.5. The entity-entry Group

The CDDL for the entity-entry group follows:

entity-entry = {
    global-attributes,  
    entity-name => text, 
    ? reg-id => any-uri, 
    role => $role / [ 2* $role ], 
    ? thumbprint => hash-entry, 
    * $$entity-extension, 
}
entity-name = 31
reg-id = 32
role = 33
thumbprint = 34

$role /= tag-creator
$role /= software-creator
$role /= aggregator
$role /= distributor
$role /= licensor
$role /= uint / text
  tag-creator=1
  software-creator=2
  aggregator=3
  distributor=4
  licensor=5

The following describes each child item of this group.

- global-attributes: The global-attributes group described in Section 2.4.

- entity-name (index 32): The textual name of the organizational entity claiming the roles specified by the role item for the CoSWID tag.

- reg-id (index 32): The registration id value is intended to uniquely identify a naming authority in a given scope (e.g. global, organization, vendor, customer, administrative domain, etc.) for the referenced entity. The value of an registration ID MUST be a RFC 3986 URI. The scope SHOULD be the scope of an organization. In a given scope, the registration id MUST be used consistently for CoSWID tag production.

- role (index 33): The relationship(s) between the entity, and this tag or the referenced software component. Use of index values
instead of text for these pre-defined roles allows a CoSWID to be more concise.

An initial set of pre-defined role index and text values are defined in Section 4.2 that are based on the roles defined in [SWID]. These pre-defined roles are registered with IANA in the "SWID/CoSWID Entity Role Value" registry Section 5.2.2, and MAY be expanded in the future.

The value of a role item MUST be one of the following:

* The index (preferred) or string value of a role from the IANA in the "SWID/CoSWID Entity Role Value" registry.

* An index value in the range 128 through 255, to indicate that a private use index value is used.

* A string value prefixed with "x_", to indicate that a private use string value is used.

The following additional requirements exist for the use of the "role" item:

* An entity item MUST be provided with the role of "tag-creator" for every CoSWID tag. This indicates the organization that created the CoSWID tag.

* An entity item SHOULD be provided with the role of "software-creator" for every CoSWID tag, if this information is known to the tag creator. This indicates the organization that created the referenced software component.

  o thumbprint (index 34): The value of the thumbprint item provides an integer-based hash algorithm identifier (hash-alg-id) and a byte string value (hash-value) that contains the corresponding hash value (i.e. the thumbprint) of the signing entity’s public key certificate. This provides an indicator of which entity signed the CoSWID tag, which will typically be the tag creator. If the hash-alg-id is not known, then the integer value "0" MUST be used. This ensures parity between the SWID tag specification [SWID], which does not allow an algorithm to be identified for this field. See Section 2.8.1 for more details on the use of the hash-entry data structure.

  o $entity-extension: This CDDL socket can be used to extend the entity-entry group model. See Section 2.1.
2.6. The link-entry Map

The CDDL for the link-entry map follows:

```
link-entry = {
  global-attributes,
  ? artifact => text,
  href => any-uri,
  ? media => text,
  ? ownership => $ownership,
  rel => $rel,
  ? media-type => text,
  ? use => $use,
  * $$link-extension,
}
```

```
media = 10
artifact = 37
href = 38
ownership = 39
rel = 40
media-type = 41
use = 42
```

```
$ownership /= shared
$ownership /= private
$ownership /= abandon
$ownership /= uint / text
shared=1
private=2
abandon=3
```

```
$rel /= ancestor
$rel /= component
$rel /= feature
$rel /= installationmedia
$rel /= packageinstaller
$rel /= parent
$rel /= patches
$rel /= requires
$rel /= see-also
$rel /= supersedes
$rel /= supplemental
$rel /= uint / text
ancestor=1
component=2
feature=3
installationmedia=4
packageinstaller=5
```

The following describes each member of this map.

- global-attributes: The global-attributes group described in Section 2.4.

- artifact (index: 37): To be used with rel="installation-media", this item value can provide the path to the installer executable or script that can be run to launch the referenced installation. Links with the same artifact name MUST be considered mirrors of each other, allowing the installation media to be acquired from any of the described sources.

- href (index 38): A URI for the referenced resource. The "href" item’s value can be, but is not limited to, the following (which is a slightly modified excerpt from [SWID]):
  
  * If no URI scheme is provided, then the URI is to be interpreted as being relative to the URI of the CoSWID tag. For example, "./folder/supplemental.coswid".
  
  * a physical resource location with any acceptable URI scheme (e.g., file:// http:// https:// ftp://)
  
  * a URI with "coswid:" as the scheme, which refers to another CoSWID by tag-id. This URI would need to be resolved in the context of the endpoint by software that can lookup other CoSWID tags. For example, "coswid:2df9de35-0aff-4a86-ace6-f7d3dd1ade4c" references the tag with the tag-id value "2df9de35-0aff-4a86-ace6-f7d3dd1ade4c".

  * a URI with "swidpath:" as the scheme, which refers to another CoSWID via an XPATH query. This URI would need to be resolved in the context of the system entity via software components
that can lookup other CoSWID tags and select the appropriate
tag based on an XPATH query [W3C.REC-xpath20-20101214].
Examples include:

*   swidpath://SoftwareIdentity[Entity/@regid='http://contoso.com']
    would retrieve all CoSWID tags that include an entity where the
    regid is "Contoso" or swidpath://SoftwareIdentity[Meta/@persist
    entId='b0c55172-38e9-4e36-be86-92206ad8eddb'] would match
    CoSWID tags with the persistent-id value
    "b0c55172-38e9-4e36-be86-92206ad8eddb".

o  media (index 10): A hint to the consumer of the link to what the
target item is applicable for. This item represents a query as
declared by the W3C Media Queries Recommendation (see
[W3C.REC-css3-mediaqueries-20120619]). See also media defined in
Section 2.2.

o  ownership (index 39): Used when the "href" item references another
software component to indicate the degree of ownership between the
software component referenced by the COSWID tag and the software
component referenced by the link.

An initial set of pre-defined ownership index and text values are
defined in Section 4.3 that are based on the ownership values
defined in [SWID]. These pre-defined ownership values are
registered with IANA in the "SWID/CoSWID Link Ownership Value"
registry Section 5.2.3, and MAY be expanded in the future.

The value of an ownership item MUST be one of the following:

*   The index (preferred) or string value of a role from the IANA
    in the "SWID/CoSWID Link Ownership Value" registry.

*   An index value in the range 128 through 255, to indicate that a
    private use index value is used.

*   A string value prefixed with "x_", to indicate that a private
    use string value is used.

o  rel (index 40): Identifies the relationship between this CoSWID
and the target resource indicated by the "href" item.

An initial set of pre-defined rel index and text values are
defined in Section 4.4 that are based on the rel values defined in
[SWID]. These pre-defined rel values are registered with IANA in
the "SWID/CoSWID Link Relationship Value" registry Section 5.2.4,
and MAY be expanded in the future.
The value of a rel item MUST be one of the following:

* The index (preferred) or string value of a role from the IANA in the "SWID/CoSWID Link Relationship Value" registry.

* An index value in the range 128 through 255, to indicate that a private use index value is used.

* A string value prefixed with "x_", to indicate that a private use string value is used.

* A string value, as defined by [RFC8288], corresponding to a "Relation Name" from the IANA "Link Relation Types" registry: https://www.iana.org/assignments/link-relations/link-relations.xhtml. When a string value defined in the IANA "SWID/CoSWID Link Relationship Value" registry matches a Relation Name defined in the IANA "Link Relation Types" registry, the value in the IANA "SWID/CoSWID Link Relationship Value" registry MUST be used instead, as this relationship has a specialized meaning in the context of a SWID/CoSWID tag.

- media-type (index 41): The media type for the target resource, providing a resource consumer with a hint of what type of resource to expect. Media types are identified by referencing a "Name" from the IANA "Media Types" registry: http://www.iana.org/assignments/media-types/media-types.xhtml.

- use (index 42): Determines if the referenced software component has to be installed before installing the tagged software component.

An initial set of pre-defined use index and text values are defined in Section 4.5 that are based on the use values defined in [SWID]. These pre-defined use values are registered with IANA in the "SWID/CoSWID Link Use Value" registry Section 5.2.5, and MAY be expanded in the future.

The value of an ownership item MUST be one of the following:

* The index (preferred) or string value of a role from the IANA in the "SWID/CoSWID Link Use Value" registry.

* An index value in the range 128 through 255, to indicate that a private use index value is used.

* A string value prefixed with "x_", to indicate that a private use string value is used.
2.7. The software-meta-entry Map

The CDDL for the software-meta-entry map follows:

```cddl
software-meta-entry = {
    global-attributes,
    ? activation-status => text,
    ? channel-type => text,
    ? colloquial-version => text,
    ? description => text,
    ? edition => text,
    ? entitlement-data-required => bool,
    ? entitlement-key => text,
    ? generator => text,
    ? persistent-id => text,
    ? product => text,
    ? product-family => text,
    ? revision => text,
    ? summary => text,
    ? unspsc-code => text,
    ? unspsc-version => text,
    * $$meta-extension,
}
```

activation-status = 43
channel-type = 44
colloquial-version = 45
description = 46
edition = 47
entitlement-data-required = 48
entitlement-key = 49
generator = 50
persistent-id = 51
product = 52
product-family = 53
revision = 54
summary = 55
unspsc-code = 56
unspsc-version = 57

The following describes each child item of this group.

- global-attributes: The global-attributes group described in Section 2.4.
- **activation-status (index 43):** A textual value that identifies how the software component has been activated, which might relate to specific terms and conditions for its use (e.g. Trial, Serialized, Licensed, Unlicensed, etc) and relate to an entitlement. This attribute is typically used in supplemental tags as it contains information that might be selected during a specific install.

- **channel-type (index 44):** A textual value that identifies which sales, licensing, or marketing channel the software component has been targeted for (e.g. Volume, Retail, OEM, Academic, etc). This attribute is typically used in supplemental tags as it contains information that might be selected during a specific install.

- **colloquial-version (index 45):** A textual value for the software component's informal or colloquial version. Examples may include a year value, a major version number, or similar value that are used to identify a group of specific software component releases that are part of the same release/support cycle. This version can be the same through multiple releases of a software component, while the software-version specified in the concise-swid-tag group is much more specific and will change for each software component release. This version is intended to be used for string comparison only, and is not intended to be used to determine if a specific value is earlier or later in a sequence.

- **description (index 46):** A textual value that provides a detailed description of the software component, which can be multiple sentences.

- **edition (index 47):** A textual value indicating that the software component represents a functional variation of the code base used to support multiple software components. For example, this item can be used to differentiate enterprise, standard, or professional variants of a software component.

- **entitlement-data-required (index 48):** A boolean value that proof of indicator to determine if accompanying proof of entitlement is needed when a software license reconciliation process is performed.

- **entitlement-key (index 49):** A vendor-specific textual key that can be used to identify and establish a relationship to an entitlement. Examples of an entitlement-key might include a serial number, product key, or license key. For values that relate to a given software component install (i.e., license key), a supplemental tag will typically contain this information. In
other cases where a general-purpose key can be provided that applies to all possible installs of the software component on different endpoints, a primary tag will typically contain this information.

- **generator (index 50):** The name (or tag-id) of the software component that created the CoSWID tag. If the generating software component has a SWID or CoSWID tag, then the tag-id for the generating software component SHOULD be provided.

- **persistent-id (index 51):** A GUID used to identify a related set of software components. Software components sharing the same persistent-id can be different versions.

- **product (index 52):** A basic name for the software component that can be common across multiple tagged software components (e.g., Apache HTTPD).

- **product-family (index 53):** A textual value indicating the software components overall product family. This should be used when multiple related software components form a larger capability that is installed on multiple different endpoints. For example, some software families may consist of server, client, and shared service components that are part of a larger capability. Email systems, enterprise applications, backup services, web conferencing, and similar capabilities are examples of families.

- **revision (index 54):** A string value indicating an informal or colloquial release version of the software. This value can provide a different version value as compared to the software-version specified in the concise-swid-tag group. This is useful when one or more releases need to have an informal version label that differs from the specific exact version value specified by software-version. Examples can include SP1, RC1, Beta, etc.

- **summary (index 55):** A short description of the software component. This MUST be a single sentence suitable for display in a user interface.

- **unspsc-code (index 56):** An 8 digit UNSPSC classification code for the software component. For more information see, http://www.unspsc.org/.

- **unspsc-version (index 57):** The version of UNSPSC used to define the unspsc-code value.

- **$meta-extension:** This CDDL socket can be used to extend the software-meta-entry group model. See Section 2.1.
2.8. The Resource Collection Definition

2.8.1. The hash-entry Array

CoSWID adds explicit support for the representation of hash entries using algorithms that are registered in the IANA "Named Information Hash Algorithm Registry" using the hash-entry member (label 58).

hash-entry = [ hash-alg-id: int, hash-value: bytes ]

The number used as a value for hash-alg-id MUST refer an ID in the "Named Information Hash Algorithm Registry" (see https://www.iana.org/assignments/named-information/named-information.xhtml); other hash algorithms MUST NOT be used. The hash-value MUST represent the raw hash value of the hashed resource generated using the hash algorithm indicated by the hash-alg-id.

2.8.2. The resource-collection Group

A list of items both used in evidence (created by a software discovery process) and payload (installed in an endpoint) content of a CoSWID tag document to structure and differentiate the content of specific CoSWID tag types. Potential content includes directories, files, processes, or resources.

The CDDL for the resource-collection group follows:


filesystem-item = ( global-attributes, ? key => bool, ? location => text, fs-name => text, ? root => text, )

path-elements-entry = [ [ * file-entry ], [ * directory-entry ], ]

file-entry = ( filesystem-item, }
? size => integer,
? file-version => text,
? hash => hash-entry,
* $$file-extension
}

directory-entry = {
  filesystem-item,
  path-elements => path-elements-entry,
  * $$directory-extension
}

process-entry = {
  global-attributes,
  process-name => text,
  ? pid => integer,
  * $$process-extension
}

resource-entry = {
  global-attributes,
  type => text,
  * $$resource-extension
}

directory = 16
file = 17
process = 18
resource = 19
size = 20
file-version = 21
key = 22
location = 23
fs-name = 24
root = 25
path-elements = 26
process-name = 27
pid = 28
type = 29

The following describes each member of the groups and maps illustrated above.

  o filesystem-item: A list of items both used in representing the
    nodes of a file-system hierarchy (i.e., directory items that allow
    one or more directories to be defined in the file structure), and
    file items that allow one or more files to be specified for a
given location.
o global-attributes: The global-attributes group described in Section 2.4.

o directory (index 16): A directory item allows child directory and file items to be defined within a directory hierarchy for the software component.

o file (index 17): A file item allows details about a file to be provided for the software component.

o process (index 18): A process item allows details to be provided about the runtime behavior of the software component, such as information that will appear in a process listing on a device.

o resource (index 19): A resource item can be used to provide details about a resource expected to be found on an endpoint, or evidence collected related to the software component.

o size (index 20): The file’s size in bytes.

o file-version (index 21): The file’s version as reported by querying information on the file from the operating system.

o key (index 22): A boolean value indicating if a file or directory is significant or required for the software component to execute or function properly. These are files or directories that can be used to affirmatively determine if the software component is installed on an endpoint.

o location (index 23): The filesystem path where a file is expected to be located when installed or copied. This path SHOULD be relative to the location of the parent directory item, or if no parent is defined, the location MUST be relative to the location of the CoSWID tag. The location MUST not include a file’s name, which is provided by the fs-name item.

o fs-name (index 24): The name of the directory or file without any path information.

o root (index 25): A filesystem-specific name for the root of the filesystem. The location item is considered relative to this location if specified. If not provided, the value provided by the location item is expected to be relative to its parent or the location of the CoSWID tag if no parent is provided.

o path-elements (index 26): This group provides the ability to define a directory structure for files defined in payload or evidence items.
process-name (index 27): The software component’s process name as it will appear in an endpoint’s process list.

pid (index 28): The process ID identified for a running instance of the software component in the endpoint’s process list. This is used as part of the evidence item.

type (index 29): A string indicating the type of resource.

resource-collection-extension: This CDDL socket can be used to extend the resource-collection group model. This can be used to add new specialized types of resources. See Section 2.1.

file-extension: This CDDL socket can be used to extend the file-entry group model. See Section 2.1.

directory-extension: This CDDL socket can be used to extend the directory-entry group model. See Section 2.1.

process-extension: This CDDL socket can be used to extend the process-entry group model. See Section 2.1.

resource-extension: This CDDL socket can be used to extend the group model. See Section 2.1.

resource-extension: This CDDL socket can be used to extend the resource-entry group model. See Section 2.1.

2.8.3. The payload-entry Group

The CDDL for the payload-entry group follows:

payload-entry = {
  global-attributes,
  resource-collection,
  * $$payload-extension
}

The following describes each child item of this group.

global-attributes: The global-attributes group described in Section 2.4.

resource-collection: The resource-collection group described in Section 2.8.2.

$$payload-extension: This CDDL socket can be used to extend the payload-entry group model. See Section 2.1.
2.8.4. The evidence-entry Group

The CDDL for the evidence-entry group follows:

evidence-entry = {
  global-attributes,
  resource-collection,
  ? date => time,
  ? device-id => text,
  * $$evidence-extension
}
date = 35
device-id = 36

The following describes each child item of this group.

- global-attributes: The global-attributes group described in Section 2.4.
- resource-collection: The resource-collection group described in Section 2.8.2.
- date (index 35): The date and time the information was collected pertaining to the evidence item.
- device-id (index 36): The endpoint’s string identifier from which the evidence was collected.
- $$evidence-extension: This CDDL socket can be used to extend the evidence-entry group model. See Section 2.1.

2.9. Full CDDL Definition

In order to create a valid CoSWID document the structure of the corresponding CBOR message MUST adhere to the following CDDL data definition.

concise-swid-tag = {
  global-attributes,
  tag-id => text,
  tag-version => integer,
  ? corpus => bool,
  ? patch => bool,
  ? supplemental => bool,
  software-name => text,
  ? software-version => text,
  ? version-scheme => $version-scheme,
  ? media => text,
? software-meta => software-meta-entry / [2* software-meta-entry],
entity => entity-entry / [2* entity-entry],
? link => link-entry / [2* link-entry],
? {(( payload => payload-entry ) // ( evidence => evidence-entry ))},
* $$coswid-extension
}

any-uri = text
label = text / int

$version-scheme /= multipartnumeric
$version-scheme /= multipartnumeric-suffix
$version-scheme /= alphanumeric
$version-scheme /= decimal
$version-scheme /= semver
$version-scheme /= uint / text

any-attribute = {
    label => text / int / [2* text] / [2* int]
}

global-attributes = {
? lang => text,
* any-attribute,
}

hash-entry = [hash-alg-id: int,
    hash-value: bytes,
]

directory-entry = {
    entity-name => text,
? reg-id => any-uri,
role => $role / [2* $role],
? thumbprint => hash-entry,
* $$entity-extension,
}

$role /= tag-creator
$role /= software-creator
$role /= aggregator
$role /= distributor
$role /= licensor
$role /= uint / text

link-entry = {
    global-attributes,
? artifact => text,
href => any-uri,
? media => text,
? ownership => $ownership,
rel => $rel,
? media-type => text,
? use => $use,
* $$link-extension
}

$ownership /= shared
$ownership /= private
$ownership /= abandon
$ownership /= uint / text

$rel /= ancestor
$rel /= component
$rel /= feature
$rel /= installationmedia
$rel /= packageinstaller
$rel /= parent
$rel /= patches
$rel /= requires
$rel /= see-also
$rel /= supersedes
$rel /= supplemental
$rel /= uint / text

$use /= optional
$use /= required
$use /= recommended
$use /= uint / text

software-meta-entry = {
global-attributes,
? activation-status => text,
? channel-type => text,
? colloquial-version => text,
? description => text,
? edition => text,
? entitlement-data-required => bool,
? entitlement-key => text,
? generator => text,
? persistent-id => text,
? product => text,
? product-family => text,
? revision => text,
? summary => text,
resource-collection = (  
  ? directory => directory-entry,  
  ? file => file-entry,  
  ? process => process-entry,  
  ? resource => resource-entry,  
  * $$resource-collection-extension  
)

file-entry = {  
  filesystem-item,  
  ? size => integer,  
  ? file-version => text,  
  ? hash => hash-entry,  
  * $$file-extension  
}

path-elements-entry = [  
  [ * file-entry ],  
  [ * directory-entry ],  
]

directory-entry = {  
  filesystem-item,  
  path-elements => path-elements-entry,  
  * $$directory-extension  
}

process-entry = {  
  global-attributes,  
  process-name => text,  
  ? pid => integer,  
  * $$process-extension  
}

resource-entry = {  
  global-attributes,  
  type => text,  
  * $$resource-extension  
}

filesystem-item = {  
  global-attributes,  
  ? key => bool,  
  ? location => text,  

fs-name => text,
  ? root => text,
  }

payload-entry = {
  global-attributes,
  resource-collection,
  * $$payload-extension
  }

evidence-entry = {
  global-attributes,
  resource-collection,
  ? date => time,
  ? device-id => text,
  * $$evidence-extension
  }

; "global map member" integer indexes
  tag-id = 0
  software-name = 1
  entity = 2
  evidence = 3
  link = 4
  software-meta = 5
  payload = 6
  hash = 7
  corpus = 8
  patch = 9
  media = 10
  supplemental = 11
  tag-version = 12
  software-version = 13
  version-scheme = 14
  lang = 15
  directory = 16
  file = 17
  process = 18
  resource = 19
  size = 20
  file-version = 21
  key = 22
  location = 23
  fs-name = 24
  root = 25
  path-elements = 26
  process-name = 27
  pid = 28
type = 29
entity-name = 31
reg-id = 32
role = 33
thumbprint = 34
date = 35
device-id = 36
artifact = 37
href = 38
ownership = 39
rel = 40
media-type = 41
use = 42
activation-status = 43
channel-type = 44
colloquial-version = 45
description = 46
description = 46
description = 46
description = 46
description = 46
description = 46
description = 46
edition = 47
entitlement-data-required = 48
entitlement-key = 49
generator = 50
persistent-id = 51
product = 52
product-family = 53
revision = 54
summary = 55
unspsc-code = 56
unspsc-version = 57

; "version-scheme" integer indexes
multipartnumeric = 1
multipartnumeric-suffix = 2
alphanumeric = 3
decimal = 4
semver = 16384

; "role" integer indexes
tag-creator=1
software-creator=2
aggregator=3
distributor=4
licensor=5

; ownership integer indexes
shared=1
private=2
abandon=3
3. Determining the Type of CoSWID

The operational model for SWID and CoSWID tags was introduced in Section 1.1, which described four different CoSWID tag types. The following additional rules apply to the use of CoSWID tags to ensure that created tags properly identify the tag type.

The first matching rule MUST determine the type of the CoSWID tag.

1. Primary Tag: A CoSWID tag MUST be considered a primary tag if the corpus, patch, and supplemental items are "false".

2. Supplemental Tag: A CoSWID tag MUST be considered a supplemental tag if the supplemental item is set to "true".

3. Corpus Tag: A CoSWID tag MUST be considered a corpus tag if the corpus item is "true".

4. Patch Tag: A CoSWID tag MUST be considered a patch tag if the patch item is "true".

4. CoSWID Indexed Label Values

4.1. Version Scheme

The following table contains a set of values for use in the concise-swid-tag group’s version-scheme item. These values match the version schemes defined in the ISO/IEC 19770-2:2015 [SWID] specification. Index value indicates the value to use as the version-scheme item’s value. The Version Scheme Name provides human-readable text for the
value. The Definition describes the syntax of allowed values for each entry.

<table>
<thead>
<tr>
<th>Index</th>
<th>Version Scheme Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>multipartnumeric</td>
<td>Numbers separated by dots, where the numbers are interpreted as integers (e.g., 1.2.3, 1.4.5, 1.2.3.4.5.6.7)</td>
</tr>
<tr>
<td>2</td>
<td>multipartnumeric+suffix</td>
<td>Numbers separated by dots, where the numbers are interpreted as integers with an additional textual suffix (e.g., 1.2.3a)</td>
</tr>
<tr>
<td>3</td>
<td>alphanumeric</td>
<td>Strictly a string, sorting is done alphanumerically</td>
</tr>
<tr>
<td>4</td>
<td>decimal</td>
<td>A floating point number (e.g., 1.25 is less than 1.3)</td>
</tr>
<tr>
<td>16384</td>
<td>semver</td>
<td>Follows the [SEMVER] specification</td>
</tr>
</tbody>
</table>

The values above are registered in the IANA "SWID/CoSWID Version Scheme Value" registry defined in section Section 5.2.1. Additional entries will likely be registered over time in this registry. Additionally, the index values 32768 through 65535 have been reserved for private use.

4.2. Entity Role Values

The following table indicates the index value to use for the entity-entry group’s role item (see Section 2.5). These values match the entity roles defined in the ISO/IEC 19770-2:2015 [SWID] specification. The "Index" value indicates the value to use as the role item’s value. The "Role Name" provides human-readable text for the value. The "Definition" describes the semantic meaning of each entry.
<table>
<thead>
<tr>
<th>Index</th>
<th>Role Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>tagCreator</td>
<td>The person or organization that created the containing SWID or CoSWID tag</td>
</tr>
<tr>
<td>2</td>
<td>softwareCreator</td>
<td>From [SAM], &quot;person or organization that creates a software product (3.46) or package&quot;</td>
</tr>
<tr>
<td>3</td>
<td>aggregator</td>
<td>From {{SWID}, &quot;An organization or system that encapsulates software from their own and/or other organizations into a different distribution process (as in the case of virtualization), or as a completed system to accomplish a specific task (as in the case of a value added reseller).&quot;}</td>
</tr>
<tr>
<td>4</td>
<td>distributor</td>
<td>From [SWID], &quot;An entity that furthers the marketing, selling and/or distribution of software from the original place of manufacture to the ultimate user without modifying the software, its packaging or its labelling.&quot;</td>
</tr>
<tr>
<td>5</td>
<td>licensor</td>
<td>From [SAM] as &quot;software licensor&quot;, a &quot;person or organization who owns or holds the rights to issue a software license for a specific software package&quot;</td>
</tr>
</tbody>
</table>

The values above are registered in the IANA "SWID/CoSWID Entity Role Value" registry defined in section Section 5.2.2. Additional valid values will likely be registered over time. Additionally, the index values 128 through 255 have been reserved for private use.

4.3. Link Ownership Values

The following table indicates the index value to use for the link-entry group’s ownership item (see Section 2.6). These values match the link ownership values defined in the ISO/IEC 19770-2:2015 [SWID] specification. The "Index" value indicates the value to use as the link-entry group ownership item’s value. The "Ownership Type" provides human-readable text for the value. The "Definition" describes the semantic meaning of each entry.
### Ownership Type Definition

1. **abandon**
   - If the software component referenced by the CoSWID tag is uninstalled, then the referenced software SHOULD not be uninstalled.

2. **private**
   - If the software component referenced by the CoSWID tag is uninstalled, then the referenced software SHOULD be uninstalled as well.

3. **shared**
   - If the software component referenced by the CoSWID tag is uninstalled, then the referenced software SHOULD be uninstalled if no other components sharing the software.

The values above are registered in the IANA "SWID/CoSWID Link Ownership Value" registry defined in section Section 5.2.3. Additional valid values will likely be registered over time. Additionally, the index values 128 through 255 have been reserved for private use.

### 4.4. Link Rel Values

The following table indicates the index value to use for the link-entry group’s rel item (see Section 2.6). These values match the link rel values defined in the ISO/IEC 19770-2:2015 [SWID] specification. The "Index" value indicates the value to use as the link-entry group ownership item’s value. The "Relationship Type" provides human-readable text for the value. The "Definition" describes the semantic meaning of each entry.

<table>
<thead>
<tr>
<th>Index</th>
<th>Relationship Type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ancestor</td>
<td>The link references a SWID/CoSWID tag for an ancestor of this software. This can be useful to define an upgrade path.</td>
</tr>
<tr>
<td>2</td>
<td>component</td>
<td>The link references a SWID/CoSWID tag for a separate component of this software.</td>
</tr>
<tr>
<td>3</td>
<td>feature</td>
<td>The link references a configurable</td>
</tr>
<tr>
<td></td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4</td>
<td>installationmedia</td>
<td>The link references the installation package that can be used to install this software.</td>
</tr>
<tr>
<td>5</td>
<td>packageinstaller</td>
<td>The link references the installation software needed to install this software.</td>
</tr>
<tr>
<td>6</td>
<td>parent</td>
<td>The link references a SWID/CoSWID tag that is the parent of this SWID/CoSWID tag.</td>
</tr>
<tr>
<td>7</td>
<td>patches</td>
<td>The link references a SWID/CoSWID tag that this software patches. Typically only used for patch SWID/CoSWID tags (see Section 1.1).</td>
</tr>
<tr>
<td>8</td>
<td>requires</td>
<td>The link references a prerequisite for installing this software. A patch SWID/CoSWID tag (see Section 1.1) can use this to represent base software or another patch that needs to be installed first.</td>
</tr>
<tr>
<td>9</td>
<td>see-also</td>
<td>The link references other software that may be of interest that relates to this software.</td>
</tr>
<tr>
<td>10</td>
<td>supersedes</td>
<td>The link references another software that this software replaces. A patch SWID/CoSWID tag (see Section 1.1) can use this to represent another patch that this patch incorporates or replaces.</td>
</tr>
<tr>
<td>11</td>
<td>supplemental</td>
<td>The link references a SWID/CoSWID tag that this tag supplements. Used on supplemental SWID/CoSWID tags (see Section 1.1).</td>
</tr>
</tbody>
</table>

The values above are registered in the IANA "SWID/CoSWID Link Relationship Value" registry defined in section Section 5.2.4. Additional valid values will likely be registered over time.
Additionally, the index values 32768 through 65535 have been reserved for private use.

4.5. Link Use Values

The following table indicates the index value to use for the link-entry group’s use item (see Section 2.6). These values match the link use values defined in the ISO/IEC 19770-2:2015 [SWID] specification. The "Index" value indicates the value to use as the link-entry group use item’s value. The "Use Type" provides human-readable text for the value. The "Definition" describes the semantic meaning of each entry.

<table>
<thead>
<tr>
<th>Index</th>
<th>Use Type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>optional</td>
<td>From [SWID], &quot;Not absolutely required; the [Link]’d software is installed only when specified.&quot;</td>
</tr>
<tr>
<td>2</td>
<td>required</td>
<td>From [SWID], &quot;The [Link]’d software is absolutely required for an operation software installation.&quot;</td>
</tr>
<tr>
<td>3</td>
<td>recommended</td>
<td>From [SWID], &quot;Not absolutely required; the [Link]’d software is installed unless specified otherwise.&quot;</td>
</tr>
</tbody>
</table>

The values above are registered in the IANA "SWID/CoSWID Link Use Value" registry defined in section Section 5.2.5. Additional valid values will likely be registered over time. Additionally, the index values 128 through 255 have been reserved for private use.

5. IANA Considerations

This document has a number of IANA considerations, as described in the following subsections.

5.1. CoSWID Items Registry

This document uses integer values as index values in CBOR maps.

This document defines a new a new registry titled "CoSWID Items". Future registrations for this registry are to be made based on [RFC8126] as follows:
<table>
<thead>
<tr>
<th>Index</th>
<th>Item Name</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>tag-id</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>1</td>
<td>software-name</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>2</td>
<td>entity</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>3</td>
<td>evidence</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>4</td>
<td>link</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>5</td>
<td>software-meta</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>6</td>
<td>payload</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>7</td>
<td>hash</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>8</td>
<td>corpus</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>9</td>
<td>patch</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>10</td>
<td>media</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>11</td>
<td>supplemental</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>12</td>
<td>tag-version</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>13</td>
<td>software-version</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>14</td>
<td>version-scheme</td>
<td>RFC-AAAA</td>
</tr>
<tr>
<td>15</td>
<td>lang</td>
<td>RFC-AAAA</td>
</tr>
</tbody>
</table>

All negative values are reserved for Private Use.

Initial registrations for the "CoSWID Items" registry are provided below. Assignments consist of an integer index value, the item name, and a reference to the defining specification.
| 16 | directory | RFC-AAAA |
| 17 | file      | RFC-AAAA |
| 18 | process   | RFC-AAAA |
| 19 | resource  | RFC-AAAA |
| 20 | size      | RFC-AAAA |
| 21 | file-version | RFC-AAAA |
| 22 | key       | RFC-AAAA |
| 23 | location  | RFC-AAAA |
| 24 | fs-name   | RFC-AAAA |
| 25 | root      | RFC-AAAA |
| 26 | path-elements | RFC-AAAA |
| 27 | process-name | RFC-AAAA |
| 28 | pid       | RFC-AAAA |
| 29 | type      | RFC-AAAA |
| 31 | entity-name | RFC-AAAA |
| 32 | reg-id    | RFC-AAAA |
| 33 | role      | RFC-AAAA |
| 34 | thumbprint | RFC-AAAA |
| 35 | date      | RFC-AAAA |
| 36 | device-id | RFC-AAAA |
| 37 | artifact  | RFC-AAAA |
| 38 | href      | RFC-AAAA |
| 39 | ownership | RFC-AAAA |
| 40 | rel       | RFC-AAAA |
5.2. SWID/CoSWID Value Registries

The following IANA registries provide a mechanism for new valid values to be added over time to common enumerations used by SWID and CoSWID.

5.2.1. SWID/CoSWID Version Scheme Value Registry

This document uses unsigned 16-bit index values to represent version-scheme item values. The initial set of version-scheme values are derived from the textual version scheme names defined in the ISO/IEC 19770-2:2015 specification [SWID].

This document defines a new registry titled "SWID/CoSWID Version Scheme Values". Future registrations for this registry are to be made based on [RFC8126] as follows:

[TO BE REMOVED: This registration should take place at the following location: https://www.iana.org/assignments/swid]

<table>
<thead>
<tr>
<th>Range</th>
<th>Registration Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-16383</td>
<td>Standards Action</td>
</tr>
<tr>
<td>16384-32767</td>
<td>Specification Required</td>
</tr>
<tr>
<td>32768-65535</td>
<td>Reserved for Private Use</td>
</tr>
</tbody>
</table>

Initial registrations for the "SWID/CoSWID Version Scheme Value" registry are provided below. Assignments consist of an integer Index value, the Version Scheme Name, and a reference to the defining specification.
5.2.2. SWID/CoSWID Entity Role Value Registry

This document uses unsigned 8-bit index values to represent entity-entry role item values. The initial set of Entity roles are derived from the textual role names defined in the ISO/IEC 19770-2:2015 specification [SWID].

This document defines a new registry titled "SWID/CoSWID Entity Role Values". Future registrations for this registry are to be made based on [RFC8126] as follows:

[TO BE REMOVED: This registration should take place at the following location: https://www.iana.org/assignments/swid]
Initial registrations for the "SWID/CoSWID Entity Role Value" registry are provided below. Assignments consist of an integer Index value, a Role Name, and a reference to the defining specification.

<table>
<thead>
<tr>
<th>Index</th>
<th>Role Name</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>tagCreator</td>
<td>See Section 4.2</td>
</tr>
<tr>
<td>2</td>
<td>softwareCreator</td>
<td>See Section 4.2</td>
</tr>
<tr>
<td>3</td>
<td>aggregator</td>
<td>See Section 4.2</td>
</tr>
<tr>
<td>4</td>
<td>distributor</td>
<td>See Section 4.2</td>
</tr>
<tr>
<td>5</td>
<td>licensor</td>
<td>See Section 4.2</td>
</tr>
<tr>
<td>6-127</td>
<td>Unassigned</td>
<td></td>
</tr>
<tr>
<td>128-255</td>
<td>Reserved for Private Use</td>
<td></td>
</tr>
</tbody>
</table>

5.2.3. SWID/CoSWID Link Ownership Value Registry

This document uses unsigned 8-bit index values to represent link-entry ownership item values. The initial set of Link ownership values are derived from the textual ownership names defined in the ISO/IEC 19770-2:2015 specification [SWID].

This document defines a new registry titled "SWID/CoSWID Link Ownership Values". Future registrations for this registry are to be made based on [RFC8126] as follows:

[TO BE REMOVED: This registration should take place at the following location: https://www.iana.org/assignments/swid]

<table>
<thead>
<tr>
<th>Range</th>
<th>Registration Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-31</td>
<td>Standards Action</td>
</tr>
<tr>
<td>32-127</td>
<td>Specification Required</td>
</tr>
<tr>
<td>128-255</td>
<td>Reserved for Private Use</td>
</tr>
</tbody>
</table>
Initial registrations for the "SWID/CoSWID Link Ownership Value" registry are provided below. Assignments consist of an integer Index value, an Ownership Type Name, and a reference to the defining specification.

<table>
<thead>
<tr>
<th>Index</th>
<th>Ownership Type Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>abandon</td>
<td>See Section 4.3</td>
</tr>
<tr>
<td>2</td>
<td>private</td>
<td>See Section 4.3</td>
</tr>
<tr>
<td>3</td>
<td>shared</td>
<td>See Section 4.3</td>
</tr>
<tr>
<td>4-16384</td>
<td>Unassigned</td>
<td></td>
</tr>
<tr>
<td>16385-32767</td>
<td>Unassigned</td>
<td></td>
</tr>
<tr>
<td>32768-65535</td>
<td>Reserved for Private Use</td>
<td></td>
</tr>
</tbody>
</table>

5.2.4. SWID/CoSWID Link Relationship Value Registry

This document uses unsigned 16-bit index values to represent link-entry rel item values. The initial set of rel values are derived from the textual rel names defined in the ISO/IEC 19770-2:2015 specification [SWID].

This document defines a new registry titled "SWID/CoSWID Link Relationship Values". Future registrations for this registry are to be made based on [RFC8126] as follows:

[TO BE REMOVED: This registration should take place at the following location: https://www.iana.org/assignments/swid]

<table>
<thead>
<tr>
<th>Range</th>
<th>Registration Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-16383</td>
<td>Standards Action</td>
</tr>
<tr>
<td>16384-32767</td>
<td>Specification Required</td>
</tr>
<tr>
<td>32768-65535</td>
<td>Reserved for Private Use</td>
</tr>
</tbody>
</table>
Initial registrations for the "SWID/CoSWID Link Relationship Value" registry are provided below. Assignments consist of an integer Index value, the Relationship Type Name, and a reference to the defining specification.

<table>
<thead>
<tr>
<th>Index</th>
<th>Relationship Type Name</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>ancestor</td>
<td>See Section 4.4</td>
</tr>
<tr>
<td>2</td>
<td>component</td>
<td>See Section 4.4</td>
</tr>
<tr>
<td>3</td>
<td>feature</td>
<td>See Section 4.4</td>
</tr>
<tr>
<td>4</td>
<td>installationmedia</td>
<td>See Section 4.4</td>
</tr>
<tr>
<td>5</td>
<td>packageinstaller</td>
<td>See Section 4.4</td>
</tr>
<tr>
<td>6</td>
<td>parent</td>
<td>See Section 4.4</td>
</tr>
<tr>
<td>7</td>
<td>patches</td>
<td>See Section 4.4</td>
</tr>
<tr>
<td>8</td>
<td>requires</td>
<td>See Section 4.4</td>
</tr>
<tr>
<td>9</td>
<td>see-also</td>
<td>See Section 4.4</td>
</tr>
<tr>
<td>10</td>
<td>supersedes</td>
<td>See Section 4.4</td>
</tr>
<tr>
<td>11</td>
<td>supplemental</td>
<td>See Section 4.4</td>
</tr>
<tr>
<td>12-16384</td>
<td>Unassigned</td>
<td></td>
</tr>
<tr>
<td>16385-32767</td>
<td>Unassigned</td>
<td></td>
</tr>
<tr>
<td>32768-65535</td>
<td>Reserved for Private Use</td>
<td></td>
</tr>
</tbody>
</table>

5.2.5. SWID/CoSWID Link Use Value Registry

This document uses unsigned 8-bit index values to represent link-entry use item values. The initial set of Link use values are derived from the textual names defined in the ISO/IEC 19770-2:2015 specification [SWID].
This document defines a new registry titled "SWID/CoSWID Link Use Values". Future registrations for this registry are to be made based on [RFC8126] as follows:

[TO BE REMOVED: This registration should take place at the following location: https://www.iana.org/assignments/swid]

<table>
<thead>
<tr>
<th>Range</th>
<th>Registration Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-31</td>
<td>Standards Action</td>
</tr>
<tr>
<td>32-127</td>
<td>Specification Required</td>
</tr>
<tr>
<td>128-255</td>
<td>Reserved for Private Use</td>
</tr>
</tbody>
</table>

Initial registrations for the "SWID/CoSWID Entity Role Value" registry are provided below. Assignments consist of an integer Index value, the Link Use Type Name, and a reference to the defining specification.

<table>
<thead>
<tr>
<th>Index</th>
<th>Link Use Type Name</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>optional</td>
<td>See Section 4.5</td>
</tr>
<tr>
<td>2</td>
<td>required</td>
<td>See Section 4.5</td>
</tr>
<tr>
<td>3</td>
<td>recommended</td>
<td>See Section 4.5</td>
</tr>
<tr>
<td>4-127</td>
<td>Unassigned</td>
<td></td>
</tr>
<tr>
<td>128-255</td>
<td>Reserved for Private Use</td>
<td></td>
</tr>
</tbody>
</table>

5.3. swid+cbor Media Type Registration

IANA is requested add the following to the IANA "Media Types" registry.

Type name: application

Subtype name: swid+cbor

Required parameters: none
Optional parameters: none

Encoding considerations: Must be encoded as using [RFC7049]. See RFC-AAAA for details.

Security considerations: See Section 6 of RFC-AAAA.

Interoperability considerations: Applications MAY ignore any key value pairs that they do not understand. This allows backwards compatible extensions to this specification.

Published specification: RFC-AAAA

Applications that use this media type: The type is used by Software asset management systems, Vulnerability assessment systems, and in applications that use remote integrity verification.

Fragment identifier considerations: Fragment identification for application/swid+cbor is supported by using fragment identifiers as specified by RFC-AAAA. [Section to be defined]

Additional information:

Magic number(s): first five bytes in hex: da 53 57 49 44

File extension(s): coswid

Macintosh file type code(s): none

Macintosh Universal Type Identifier code: org.ietf.coswid conforms to public.data

Person & email address to contact for further information: Henk Birkholz <henk.birkholz@sit.fraunhofer.de>

Intended usage: COMMON

Restrictions on usage: None

Author: Henk Birkholz <henk.birkholz@sit.fraunhofer.de>

Change controller: IESG

5.4. CoAP Content-Format Registration

IANA is requested to assign a CoAP Content-Format ID for the CoSWID media type in the "CoAP Content-Formats" sub-registry, from the "IETF
Review or IESG Approval space (256..999), within the "CoRE Parameters" registry [RFC7252]:

<table>
<thead>
<tr>
<th>Media type</th>
<th>Encoding</th>
<th>ID</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>application/swid+cbor</td>
<td>-</td>
<td>TBD1</td>
<td>RFC-AAAA</td>
</tr>
</tbody>
</table>

Table 1: CoAP Content-Format IDs

5.5. CBOR Tag Registration

IANA is requested to allocate a tag in the "CBOR Tags" registry", preferably with the specific value requested:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Data Item</th>
<th>Semantics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1398229316</td>
<td>map</td>
<td>Concise Software Identifier (CoSWID)  [RFC-AAAA]</td>
</tr>
</tbody>
</table>

6. Security Considerations

SWID and CoSWID tags contain public information about software components and, as such, do not need to be protected against disclosure on an endpoint. Similarly, SWID tags are intended to be easily discoverable by applications and users on an endpoint in order to make it easy to identify and collect all of an endpoint’s SWID tags. As such, any security considerations regarding SWID tags focus on the application of SWID tags to address security challenges, and the possible disclosure of the results of those applications.

A signed SWID tag whose signature has been validated can be relied upon to be unchanged since it was signed. If the SWID tag was created by the software provider, is signed, and the software provider can be authenticated as the originator of the signature, then the tag can be considered authoritative. In this way, an authoritative SWID tag contains information about a software product provided by the maintainer of the product, who is expected to be an expert in their own product. Thus, authoritative SWID tags can be trusted to represent authoritative information about the software product. Having an authoritative SWID tag can be useful when the information in the tag needs to be trusted, such as when the tag is being used to convey reference integrity measurements for software
SWID tags are designed to be easily added and removed from an endpoint along with the installation or removal of software components. On endpoints where addition or removal of software components is tightly controlled, the addition or removal of SWID tags can be similarly controlled. On more open systems, where many users can manage the software inventory, SWID tags can be easier to add or remove. On such systems, it can be possible to add or remove SWID tags in a way that does not reflect the actual presence or absence of corresponding software components. Similarly, not all software products automatically install SWID tags, so products can be present on an endpoint without providing a corresponding SWID tag. As such, any collection of SWID tags cannot automatically be assumed to represent either a complete or fully accurate representation of the software inventory of the endpoint. However, especially on devices that more strictly control the ability to add or remove applications, SWID tags are an easy way to provide an preliminary understanding of that endpoint’s software inventory.

Any report of an endpoint’s SWID tag collection provides information about the software inventory of that endpoint. If such a report is exposed to an attacker, this can tell them which software products and versions thereof are present on the endpoint. By examining this list, the attacker might learn of the presence of applications that are vulnerable to certain types of attacks. As noted earlier, SWID tags are designed to be easily discoverable by an endpoint, but this does not present a significant risk since an attacker would already need to have access to the endpoint to view that information. However, when the endpoint transmits its software inventory to another party, or that inventory is stored on a server for later analysis, this can potentially expose this information to attackers who do not yet have access to the endpoint. For this reason, it is important to protect the confidentiality of SWID tag information that has been collected from an endpoint, not because those tags individually contain sensitive information, but because the collection of SWID tags and their association with an endpoint reveals information about that endpoint’s attack surface.

Finally, both the ISO-19770-2:2015 XML schema definition and the Concise SWID data definition allow for the construction of "infinite" SWID tags or SWID tags that contain malicious content with the intent of creating non-deterministic states during validation or processing of SWID tags. While software product vendors are unlikely to do this, SWID tags can be created by any party and the SWID tags collected from an endpoint could contain a mixture of vendor and non-vendor created tags. For this reason, tools that consume SWID tags
ought to treat the tag contents as potentially malicious and employ input sanitizing on the tags they ingest.

7. Acknowledgments

TBD

8. Change Log

Changes from version 03 to version 09:

- Reduced representation complexity of the media-entry type and removed the section describing the older data structure.
- Added more signature schemes from COSE
- Included a minimal required set of normative language
- Reordering of attribute name to integer label by priority according to semantics.
- Added an IANA registry for CoSWID items supporting future extension.
- Cleaned up IANA registrations, fixing some inconsistencies in the table labels.
- Added additional CDDL sockets for resource collection entries providing for additional extension points to address future SWID/CoSWID extensions.
- Updated section on extension points to address new CDDL sockets and to reference the new IANA registry for items.
- Removed unused references and added new references to address placeholder comments.
- Added table with semantics for the link ownership item.
- Clarified language, made term use more consistent, fixed references, and replacing lowercase RFC2119 keywords.

Changes from version 02 to version 03:

- Updated core CDDL including the CDDL design pattern according to RFC 8428.

Changes from version 01 to version 02:
Enforced a more strict separation between the core CoSWID definition and additional usage by moving content to corresponding appendices.

- Removed artifacts inherited from the reference schema provided by ISO (e.g. NMTOKEN(S))

- Simplified the core data definition by removing group and type choices where possible

- Minor reordering of map members

- Added a first extension point to address requested flexibility for extensions beyond the any-element

Changes from version 00 to version 01:

- Ambiguity between evidence and payload eliminated by introducing explicit members (while still allowing for "empty" SWID tags)

- Added a relatively restrictive COSE envelope using cose_sign1 to define signed CoSWID (single signer only, at the moment)

- Added a definition how to encode hashes that can be stored in the any-member using existing IANA tables to reference hash-algorithms

Changes since adopted as a WG I-D -00:

- Removed redundant any-attributes originating from the ISO-19770-2:2015 XML schema definition

- Fixed broken multi-map members

- Introduced a more restrictive item (any-element-map) to represent custom maps, increased restriction on types for the any-attribute, accordingly

- Fixed X.1520 reference

- Minor type changes of some attributes (e.g. NMTOKENS)

- Added semantic differentiation of various name types (e.g. fs-name)

Changes from version 06 to version 07:
o Added type choices/enumerations based on textual definitions in 19770-2:2015
o Added value registry request
o Added media type registration request
o Added content format registration request
o Added CBOR tag registration request
o Removed RIM appendix to be addressed in complementary draft
o Removed CWT appendix
o Flagged firmware resource collection appendix for revision
o Made use of terminology more consistent
o Better defined use of extension points in the CDDL
o Added definitions for indexed values
o Added IANA registry for Link use indexed values

Changes from version 05 to version 06:

o Improved quantities
o Included proposals for implicit enumerations that were NMTOKENS
o Added extension points
o Improved exemplary firmware-resource extension

Changes from version 04 to version 05:

o Clarified language around SWID and CoSWID to make more consistent use of these terms.

o Added language describing CBOR optimizations for single vs. arrays in the model front matter.

o Fixed a number of grammatical, spelling, and wording issues.

o Documented extension points that use CDDL sockets.
o Converted IANA registration tables to markdown tables, reserving the 0 value for use when a value is not known.

o Updated a number of references to their current versions.

Changes from version 03 to version 04:

o Re-index label values in the CDDL.

o Added a section describing the CoSWID model in detail.

o Created IANA registries for entity-role and version-scheme

Changes from version 02 to version 03:

o Updated CDDL to allow for a choice between a payload or evidence

o Re-index label values in the CDDL.

o Added item definitions

o Updated references for COSE, CBOR Web Token, and CDDL.

Changes from version 01 to version 02:

o Added extensions for Firmware and CoSWID use as Reference Integrity Measurements (CoSWID RIM)

o Changes meta handling in CDDL from use of an explicit use of items to a more flexible unconstrained collection of items.

o Added sections discussing use of COSE Signatures and CBOR Web Tokens

Changes from version 00 to version 01:

o Added CWT usage for absolute SWID paths on a device

o Fixed cardinality of type-choices including arrays

o Included first iteration of firmware resource-collection

9. Contributors
10. References

10.1. Normative References


10.2. Informative References


Appendix A.  Signed Concise SWID Tags using COSE

SWID tags, as defined in the ISO-19770-2:2015 XML schema, can include cryptographic signatures to protect the integrity of the SWID tag. In general, tags are signed by the tag creator (typically, although not exclusively, the vendor of the software component that the SWID tag identifies). Cryptographic signatures can make any modification of the tag detectable, which is especially important if the integrity of the tag is important, such as when the tag is providing reference integrity measurements for files.

The ISO-19770-2:2015 XML schema uses XML DSIG to support cryptographic signatures. CoSWID tags require a different signature scheme than this. COSE (CBOR Object Signing and Encryption) provides the required mechanism [RFC8152]. Concise SWID can be wrapped in a COSE Single Signer Data Object (COSE_Sign1) that contains a single signature. The following CDDL defines a more restrictive subset of header attributes allowed by COSE tailored to suit the requirements of Concise SWID tags.
signed-coswid = #6.18(COSE-Sign1-coswid)

cose-label = int / tstr
cose-values = any

protected-signed-coswid-header = {
    1 => int,                      ; algorithm identifier
    3 => "application/swid+cbor",
    * cose-label => cose-values,
}

unprotected-signed-coswid-header = {
    4 => bstr,                     ; key identifier
    * cose-label => cose-values,
}

COSE-Sign1-coswid = [
    protected: bstr .cbor protected-signed-coswid-header,
    unprotected: unprotected-signed-coswid-header,
    payload: bstr .cbor concise-swid-tag,
    signature: bstr,
]

Optionally, the COSE_Sign structure that allows for more than one
signature to be applied to a CoSWID tag MAY be used. The
corresponding usage scenarios are domain-specific and require well-
declared application guidance. Representation of the corresponding
guidance is out-of-scope of this document.

Additionally, the COSE Header counter signature MAY be used as an
attribute in the unprotected header map of the COSE envelope of a
CoSWID. The application of counter signing enables second parties to
provide a signature on a signature allowing for a proof that a
signature existed at a given time (i.e., a timestamp).

Authors’ Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
Darmstadt  64295
Germany

Email: henk.birkholz@sit.fraunhofer.de
Jessica Fitzgerald-McKay  
Department of Defense  
9800 Savage Road  
Ft. Meade, Maryland  
USA  

Email: jmfitz2@nsa.gov

Charles Schmidt  
The MITRE Corporation  
202 Burlington Road  
Bedford, Maryland 01730  
USA  

Email: cmschmidt@mitre.org

David Waltermire  
National Institute of Standards and Technology  
100 Bureau Drive  
Gaithersburg, Maryland 20877  
USA  

Email: david.waltermire@nist.gov
Abstract

This document specifies the Endpoint Posture Collection Profile, which describes the best practices for the application of IETF, TNC, and ISO/IEC data models, protocols, and interfaces to support the on-going collection and communication of endpoint posture to a centralized server where it can be stored and made available to other tools. This document is an extension of the Trusted Computing Group’s Endpoint Compliance Profile Version 1.0 specification [ECP].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 23, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents.
carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction .................................. 4
2. Terminology .................................. 4
3. Endpoint Posture Collection Profile ............... 5
   3.1. Components .................................. 6
      3.1.1. Endpoint ................................. 7
         3.1.1.1. Posture Collection Engine ............ 7
      3.1.2. Posture Manager ......................... 8
         3.1.2.1. Posture Collection Manager ............. 8
      3.1.3. Repository .............................. 8
      3.1.4. Evaluator ................................ 9
      3.1.5. Orchestrator .............................. 9
      3.1.6. Administrative Interface and API .......... 9
   3.2. Transactions ................................ 9
      3.2.1. Provisioning ............................. 10
      3.2.2. Discovery and Validation ................. 10
      3.2.3. Event Driven Collection .................. 10
      3.2.4. Querying the Endpoint ................... 10
      3.2.5. Data Storage ............................ 10
      3.2.6. Data Sharing ............................. 11
4. IETF NEA EPCP Implementation for Traditional Endpoints ... 11
   4.1. Endpoint Provisioning ........................ 13
   4.2. Endpoint ................................... 13
      4.2.1. Posture Collector ........................ 14
      4.2.2. Posture Broker Client ................... 14
      4.2.3. Posture Transport Client .................. 14
   4.3. Posture Manager .............................. 14
      4.3.1. Posture Validator ......................... 14
      4.3.2. Posture Broker Server .................... 14
      4.3.3. Posture Transport Server .................. 14
   4.4. Repository .................................. 15
   4.5. IETF SACM SWAM Extension to the IETF NEA EPCP 
      Implementation ................................ 15
      4.5.1. Endpoint Pre-Provisioning .................. 15
      4.5.2. SWID Tags ................................ 15
      4.5.3. SWID Posture Collectors and Posture Validators ... 15
         4.5.3.1. The SWID Posture Collector .............. 16
         4.5.3.2. The SWID Posture Validator .............. 16
      4.5.4. Repository ................................ 17
5. IETF NETCONF EPCP Implementation for Network Device Endpoints 17
   5.1. Endpoint Provisioning ........................ 18
5.2. Posture Manager Provisioning .................................. 18
5.3. Endpoint ......................................................... 18
   5.3.1. datastore .................................................. 18
5.4. Posture Manager ................................................ 19
5.5. Repository ....................................................... 19
6. Future Work ....................................................... 19
7. Acknowledgements ................................................ 20
8. IANA Considerations .............................................. 22
9. Security Considerations .......................................... 22
   9.1. Threat Model .................................................. 22
      9.1.1. Endpoint Attacks ....................................... 23
      9.1.2. Network Attacks ........................................ 23
      9.1.3. Posture Manager Attacks ............................... 23
      9.1.4. Repository Attacks .................................... 24
      9.2. Countermeasures ........................................... 25
         9.2.1. Countermeasures for Endpoint Attacks ............... 25
         9.2.2. Countermeasures for Network Attacks ............... 25
         9.2.3. Countermeasures for Posture Manager Attacks ...... 26
         9.2.4. Countermeasures for Repository Attacks ............ 26
10. Privacy Considerations .......................................... 27
11. References ....................................................... 27
   11.1. Informative References ................................... 27
   11.2. Normative References ..................................... 28
Appendix A. Rationale for an EPCP Solution .......................... 30
   A.1. Preventative Posture Assessments ............................ 30
   A.2. All Network-Connected Endpoints are Endpoints .......... 31
   A.3. All Endpoints on the Network Must be Uniquely Identified 31
   A.4. Standardized Data Models .................................. 31
   A.5. Posture Information Must Be Stored ...................... 32
   A.6. Posture Information Can Be Shared ....................... 32
   A.7. Enterprise Asset Posture Information Belongs to the 32
       Enterprise ................................................... 32
Appendix B. EPCP Supported Use Cases and Non-Supported Use Cases 33
   B.1. Supported Use Cases ....................................... 33
      B.1.1. Hardware Asset Management ............................ 33
      B.1.2. Software Asset Management ............................ 33
      B.1.3. Vulnerability Management ............................. 34
      B.1.4. Threat Detection and Analysis ........................ 34
      B.2. Non-Supported Use Cases ................................ 34
Appendix C. Endpoint Posture Collection Profile Examples ............ 35
   C.1. Continuous Posture Assessment of an Endpoint ............ 35
      C.1.1. Change on Endpoint Triggers Posture Assessment ... 35
   C.2. Administrator Searches for Vulnerable Endpoints ......... 38
Appendix D. Change Log ............................................... 39
   D.1. -04 to -05 ................................................... 39
   D.2. -03 to -04 ................................................... 40
   D.3. -02 to -03 ................................................... 40
   D.4. -01 to -02 ................................................... 41

1. Introduction

The Endpoint Posture Collection Profile (EPCP) builds on prior work from the IETF NEA WG, the IETF NETCONF WG, IETF NETMOD WG, the Trusted Computing Group (TCG) Trusted Network Communications [TNC] WG, and the International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee (JTC) 1, Subcommittee (SC) 7, WG 21 (ISO/IEC JTC 1, SC7, WG21) to describe the best practices for the collection and communication of posture information from network-connected endpoints to a centralized server.

This document focuses on reducing the security exposure of a network by enabling event-driven posture collection, standardized querying of additional posture information as needed, and the communication of that data to a centralized server where it can made available to other components. Thus, eliminating the need for redundant collection and agents on endpoints. Future revisions of this document may include support for the collection of posture information from other endpoint types as well as a standardized interface for storing and querying data in repositories among other capabilities. Additional information about this future work can be found in Section 6 of this document.

To support the collection of posture information from new endpoint types, this document is organized such that it first provides a high-level overview of EPCP as well as its abstract architectural components and transactions that will be realized by implementations (Section 3). This is followed by individual sections that discuss the best practices for specific implementations of the EPCP for a given endpoint type (e.g., traditional, network device, etc.) along with any extensions for supported use cases (software asset management, vulnerability management, etc.).

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]. 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.

Furthermore, this document uses terms as defined in [I-D.ietf-sacm-terminology] unless otherwise specified.

3. Endpoint Posture Collection Profile

The EPCP describes how IETF, TCG, and ISO/IEC data models, protocols, and interfaces can be used to support the posture assessment of endpoints on a network. This profile does not generate new data models, protocols, or interfaces; rather, it offers best practices for a full end-to-end solution for posture assessment, as well as a fresh perspective on how existing standards can be leveraged against vulnerabilities. Rationale for the EPCP solution as well as the supported and non-supported use cases is available in Appendix A and Appendix B respectively.

The EPCP makes it possible to perform posture assessments against all network-connected endpoints by:

1. uniquely identifying the endpoint;

2. collecting and evaluating posture based on data from the endpoint (asset management, software asset management, vulnerability management, and configuration management);

3. creating a secure, authenticated, confidential channel between the endpoint and the posture manager;

4. enabling the endpoint to notify the posture manager about changes to its configuration;

5. enabling the posture manager to request information about the configuration of the endpoint; and

6. storing the posture information in a repository linked to the identifier for the endpoint.

Furthermore, the EPCP aims to support data storage and data sharing capabilities to make the collected posture information available to authorized parties and components in support of other processes (analytic, access control, remediation, reporting, etc.).
3.1. Components

To perform posture assessment, data storage, and data sharing, the EPCP defines several components. Some of these components reside on the target endpoint. Others reside on a posture manager that manages communications with the target endpoint and stores the target endpoint's posture information in a repository.

It should be noted that the primary focus of this document is on the communication between the posture manager and endpoints. While the orchestrator, evaluator, repository, and administrative interface and API will be discussed in the context of the broader EPCP architecture, these components are not strictly defined nor are best practices provided for them at this time. As a result, vendors are free to implement these components and interfaces in a way that makes the most sense for their products.
3.1.1. Endpoint

An endpoint is defined in [RFC6876]. In the EPCP, the endpoint is monitored by the enterprise and is the target of posture assessments. To support these posture assessments, posture information is collected via a posture collection engine.

3.1.1.1. Posture Collection Engine

The posture collection engine is located on the target endpoint and can either receive queries for data from the posture collection manager (see Section 3.2.4) or can push data to the posture collection manager.
collection manager (see Section 3.2.3). The posture collection engine sends collected posture information to the posture manager.
where it can be sanity checked and stored in the repository. The posture collection engine also contains a capability that sets up exchanges between the target endpoint and posture manager. This capability makes the posture collection engine responsible for performing the client-side portion of encryption handshakes, and for locating authorized posture managers with which to communicate.

3.1.2. Posture Manager

The posture manager is an endpoint that collects, validates, and enriches posture information received about a target endpoint. It also stores the posture information it receives in the repository where it can be evaluated. The posture manager does not evaluate the posture information.

3.1.2.1. Posture Collection Manager

A posture collection manager is a lightweight and extensible component that facilitates the coordination and execution of posture collection requests using collection mechanisms deployed across the enterprise. The posture collection manager may query and retrieve guidance from the repository to guide the collection of posture information from the target endpoint.

The posture collection manager also contains a capability that sets up exchanges between the target endpoint and the posture manager, and manages data sent to and from posture collection engine. It is also responsible for performing the server-side portion of encryption handshakes.

If the posture manager wants to register for continuous collection of endpoint posture changes with the endpoint, then it must do so in a scalable way. Specifically, it will need to create subscriptions with endpoints in a way which allows the posture data to be securely pushed. Effectively this means that the endpoint must be able to establish secure transport connectivity to the posture collection manager as needed, and the collection manager must be able to periodically collect the current state of the endpoint to verify the expected state of that endpoint.

3.1.3. Repository

The repository hosts guidance, endpoint identification information, and posture information reported by target endpoints where it is made available to authorized components and persisted over a period of time set by the administrator. Information stored in the repository will be accessible to authorized parties via a standard administrative interface as well as through a standardized API.
repository may be a standalone component or may be located on the posture manager. Furthermore, an implementation is not restricted to a single repository and may leverage several repositories to provide this functionality.

3.1.4. Evaluator

The evaluator assesses the posture status of a target endpoint by comparing collected posture information against the desired state of the target endpoint specified in guidance. The evaluator queries and retrieves the appropriate guidance from the repository as well as queries and retrieves the posture information required for the assessment from the repository. If the required posture information is not available in the repository, the evaluator may request the posture information from the posture collection manager, which will result in the collection of additional posture information from the target endpoint. This information is subsequently stored in the repository where it is made available to the evaluator and other components. The results of the assessment are stored in the repository where they are available to tools and administrators for follow-up actions, further evaluation, and historical purposes.

3.1.5. Orchestrator

The orchestrator provides a publish/subscribe interface for the repository so that infrastructure endpoints can subscribe to and receive published posture assessment results from the repository regarding endpoint posture changes.

3.1.6. Administrative Interface and API

The administrative interface allows administrators to query the repository and manage the endpoints and software used in the EPCP via the posture manager. Similarly, an API is necessary to allow infrastructure endpoints and software access to the information stored in the repository and to manage the endpoints and software used in the EPCP. The administrative interface and API provide authorized users, infrastructure endpoints, and software with the ability to query the repository for data, send commands to the posture collection managers requesting information from the associated posture collection engines residing on endpoints, and establish and update the policy that resides on the posture manager.

3.2. Transactions

The following sections describe the transactions associated with the components of the EPCP architecture and may be provided in an implementation.
3.2.1. Provisioning

An endpoint is provisioned with one or more attributes that will serve as its unique identifier on the network as well as the components and data models necessary to interact with the posture manager. Examples of such identifiers include MAC addresses, serial numbers, hardware certificates compliant with [IEEE-802-1ar], and the identities of hardware cryptographic modules among others. Once provisioning is complete, the endpoint is deployed on the network. Over time, components and data models may need to be added to the endpoint or updated to support the collection needs of an enterprise.

3.2.2. Discovery and Validation

If necessary, the target endpoint finds and validates the posture manager. The posture collection engine on the target endpoint and posture collection manager on the posture manager complete an encryption handshake, during which endpoint identity information is exchanged.

3.2.3. Event Driven Collection

The posture assessment is initiated when the posture collector engine on the target endpoint notices that relevant posture information on the endpoint has changed. Then, the posture collection engine initiates a posture assessment information exchange with the posture collection manager.

3.2.4. Querying the Endpoint

The posture assessment is initiated by the posture collection manager. This can occur because:

1. policy states that a previous assessment has aged out or become invalid, or

2. the posture collection manager is alerted by a sensor or an administrator (via the posture manager’s administrative interface) that an assessment must be completed.

3.2.5. Data Storage

Once posture information is received by the posture manager, it is forwarded to the repository. The repository could be co-located with the posture manager, or there could be direct or brokered communication between the posture manager and the repository. The posture information is stored in the repository along with past posture information collected about the target endpoint.
3.2.6. Data Sharing

Because the target endpoint posture information was sent in standards-based data models over secure, standardized protocols, and then stored in a centralized repository linked to unique endpoint identifiers, authorized parties are able to access the posture information. Such authorized parties may include, but are not limited to, administrators or endpoint owners (via the posture manager’s administrative interface), evaluators that access the repository directly, and orchestrators that rely on publish/subscribe communications with the repository.

4. IETF NEA EPCP Implementation for Traditional Endpoints

When EPCP is used, posture collectors running on the target endpoint gather posture information as changes occur on the endpoint. The data is aggregated by the posture broker client and forwarded to a posture manager, over a secure channel, via the posture transport client. Once received by the posture transport server on the posture manager, the posture information is directed by the posture broker server to the appropriate posture validators where it can be processed and stored in a repository. There the posture information can be used by other tools to carry out assessment tasks. Posture collectors can also be queried by posture validators to refresh posture information about the target endpoint or to ask a specific question about posture information. This is shown in Figure 2.
These requirements are written with a view to performing a posture assessment on an endpoint; as the EPCP grows and evolves, these requirements will be expanded to address issues that arise. Note that these requirements refer to defined components of the NEA architecture [RFC5209]. As with the NEA architecture, vendors have discretion as to how these NEA components map to separate pieces of software or endpoints.

Furthermore, it should be noted that the posture broker client and posture transport client components of the posture collection engine and the posture broker server and posture transport server components of the posture collection manager would likely need to be implemented by a single vendor because there are no standardized interfaces between the respective components and would not be interoperable.

Examples of the EPCP as implemented using the components from the NEA architecture are provided in Appendix C.
4.1. Endpoint Provisioning

An endpoint is provisioned with a machine certificate that will serve as its unique identifier on the network as well as the components necessary to interact with the posture manager. This includes a posture collection engine to manage requests from the posture manager and the posture collectors necessary to collect the posture information of importance to the enterprise. The endpoint is deployed on the network.

The target endpoint SHOULD authenticate to the posture manager using a machine certificate during the establishment of the outer tunnel achieved with the posture transport protocol defined in [RFC6876]. [IF-IMV] specifies how to pull an endpoint identifier out of a machine certificate. An endpoint identifier SHOULD be created in conformance with [IF-IMV] from a machine certificate sent via [RFC6876].

In the future, the identity could be a hardware certificate compliant with [IEEE-802-1ar]; ideally, this identifier SHOULD be associated with the identity of a hardware cryptographic module, in accordance with [IEEE-802-1ar], if present on the endpoint. The enterprise SHOULD stand up a certificate root authority; install its root certificate on endpoints and on the posture manager; and provision the endpoints and the posture manager with machine certificates. The target endpoint MAY authenticate to the posture manager using a combination of the machine account and password; however, this is less secure and not recommended.

4.2. Endpoint

The endpoint MUST conform to [RFC5793], which levies several requirements against the endpoint. An endpoint that complies with these requirements will be able to:

1. attempt to initiate a session with the posture manager if the posture makes a request to send an update to posture manager;
2. notify the posture collector if no PT-TLS session with the posture manager can be created;
3. notify the posture collector when a PT-TLS session is established; and
4. receive information from the posture collectors, forward this information to the posture manager via the posture collection engine.
4.2.1. Posture Collector

Any posture collector used in an EPCP solution MUST be conformant with the TCG TNC Integrity Measurement Collector interface [IF-IMC].

4.2.2. Posture Broker Client

The posture broker client MUST conform to [IF-IMC] to enable communications between the posture broker client and the posture collectors on the endpoint.

4.2.3. Posture Transport Client

The posture transport client MUST implement PT-TLS. The posture transport client MUST support the use of machine certificates for TLS at each endpoint consistent with the requirements stipulated in [RFC6876] and [Server-Discovery]. The posture transport client MUST be able to locate an authorized posture manager, and switch to a new posture manager when required by the network, in conformance with [Server-Discovery].

4.3. Posture Manager

The posture manager MUST conform to all requirements in the [RFC5793].

4.3.1. Posture Validator

Any posture validator used in an EPCP solution MUST be conformant with the TCG TNC Integrity Measurement Verifier interface [IF-IMV].

4.3.2. Posture Broker Server

The posture broker server MUST conform to [IF-IMV]. Conformance to [IF-IMV] enables the posture broker server to obtain endpoint identity information from the posture transport server, and pass this information to any posture validators on the posture manager.

4.3.3. Posture Transport Server

The posture transport server MUST implement PT-TLS. The posture transport server MUST support the use of machine certificates for TLS at each endpoint consistent with the requirements stipulated in [RFC6876] and [Server-Discovery].
4.4. Repository

EPCP requires a simple administrative interface for the repository. Posture validators on the posture manager receive the target endpoint posture information via PA-TNC [RFC5792] messages sent from corresponding posture collectors on the target endpoint. The posture validators store this information in the repository linked to the identity of the target endpoint where the posture collectors are located.

4.5. IETF SACM SWAM Extension to the IETF NEA EPCP Implementation

This section defines the requirements associated with the software asset management extension [RFC8412] to the IETF NEA EPCP implementation.

4.5.1. Endpoint Pre-Provisioning

This section defines the requirements associated with implementing SWIMA.

The following requirements assume that the platform or OS vendor supports the use of SWID tags and has identified a standard directory location for the SWID tags to be located as specified by [SWID].

4.5.2. SWID Tags

The primary content for the EPCP is the information conveyed in the elements of a SWID tag.

The endpoint MUST have SWID tags stored in a directory specified in [SWID]. The tags SHOULD be provided by the software vendor; they MAY also be generated by:

- the software installer; or
- third-party software that creates tags based on the applications it sees installed on the endpoint.

The elements in the SWID tag MUST be populated as specified in [SWID]. These tags, and the directory in which they are stored, MUST be updated as software is added, removed, or updated.

4.5.3. SWID Posture Collectors and Posture Validators
4.5.3.1. The SWID Posture Collector

For the EPCP, the SWID posture collector MUST be conformant with [RFC8412], which includes requirements for:

1. Collecting SWID tags from the SWID directory;
2. Monitoring the SWID directory for changes;
3. Initiating a session with the posture manager to report changes to the directory;
4. Maintaining a list of changes to the SWID directory when updates take place and no PT-TLS connection can be created with the posture manager;
5. Responding to a request for SWID tags from the SWID Posture Validator on the posture manager; and
6. Responding to a query from the SWID posture validator as to whether all updates have been sent.

The SWID posture collector is not responsible for detecting that the SWID directory was not updated when an application was either installed or uninstalled.

4.5.3.2. The SWID Posture Validator

Conformance to [RFC8412] enables the SWID posture validator to:

1. Send messages to the SWID posture collector (at the behest of the administrator at the posture manager console) requesting updates for SWID tags located on endpoint;
2. Ask the SWID posture collector whether all updates to the SWID directory located at the posture manager have been sent; and
3. Perform any validation and processing on the collected SWID posture information prior to storage.

In addition to these requirements, a SWID posture validator used in conformance with this profile MUST be capable of passing this SWID posture information as well as the associated endpoint identity to the repository for storage.
4.5.4. Repository

The administrative interface SHOULD enable an administrator to:

1. Query which endpoints have reported SWID tags for a particular application
2. Query which SWID tags are installed on an endpoint; and
3. Query tags based on characteristics, such as vendor, publisher, etc.

5. IETF NETCONF EPCP Implementation for Network Device Endpoints

When EPCP is used, a NETCONF client that implements the posture collection manager sends a query to target network device endpoint requesting posture information over a secure channel. Once the NETCONF server on the endpoint receives the request, it queries one or more datastores for the posture information. The NETCONF server then reports the information back to the NETCONF client where it can be stored in a repository for use by other tools. This is shown in Figure 3.

![Figure 3: NETCONF Components](image)

These requirements are written with a view to performing a posture assessment on network device endpoints (routers, switches, etc.); as the EPCP grows and evolves, these requirements will be expanded to address issues that arise.
Note that these requirements refer to defined components of the NETCONF architecture and map back to EPCP. As with the NETCONF architecture, vendors have discretion as to how these NETCONF components map to separate pieces of software or endpoints.

5.1. Endpoint Provisioning

For the posture manager to be able to query the datastores on the endpoint, the endpoint MUST be configured to grant the posture manager access to its datastores as described in [RFC6241]. The posture manager is identified by its NETCONF username. The endpoint is deployed on the network.

5.2. Posture Manager Provisioning

For the posture manager to be able to query the datastores on the endpoint, the posture manager MUST be provisioned with a NETCONF username that will be used to authenticate the posture manager to the endpoint as described in [RFC6241]. The username generated will be determined by the selected transport protocol. The posture manager is deployed on the network.

5.3. Endpoint

An endpoint MUST conform to the requirements outlined for servers in the NETCONF protocol as defined in [RFC6241]. This requires the implementation of NETCONF over SSH [RFC6242]. An endpoint MAY support the NETCONF protocol over other transports such as TLS [RFC7589] as well as the RESTCONF protocol as defined in [RFC8040].

5.3.1. Datastore

A NETCONF datastore on an endpoint MUST support the operations outlined in [RFC6241], but, the actual implementation of the datastore is left to the endpoint vendor.

Datastores MUST support the YANG data modeling language [RFC7950] for expressing endpoint posture information in a structured format. In addition, datastores MAY support other data models such as XML (via YIN) for representing posture information.

Datastores MUST support the compliance posture information specified in [RFC7317]. Datastores MAY support other models standardized or proprietary as deemed appropriate by the endpoint vendor.
5.4. Posture Manager

A posture manager MUST conform to the requirements specified for clients in the NETCONF protocol as defined in [RFC6241]. This requires the implementation of NETCONF over SSH [RFC6242]. A posture manager MAY also support the NETCONF protocol over other transports such as TLS [RFC7589]. In addition, a posture manager MAY support the RESTCONF protocol as defined in [RFC8040].

While ad-hoc fetch/polling via NETCONF and RESTCONF is useful for assessing endpoint compliance, such solutions by themselves are not able to detect changes as they occur on the endpoint. As a result, a future revision of this document will support [I-D.ietf-netconf-yang-push] to receive updates on YANG-modeled posture information. Similarly, because not all posture information is modeled in YANG, a future revision of this document will reference [I-D.ietf-netconf-subscribed-notifications] once it is a standard to support continuous streams of unstructured data from the endpoint to the posture manager.

5.5. Repository

EPCP requires a simple administrative interface for the repository. The posture collection manager on the posture manager receives the target endpoint posture information via NETCONF [RFC6241] messages sent from posture collection engine on the target endpoint. The posture collection manager stores this information in the repository linked to the identity of the target endpoint from which it was collected.

6. Future Work

This section captures ideas for future work related to EPCP that might be of interest to the IETF SACM WG. These ideas are listed in no particular order.

- The [I-D.ietf-netconf-subscribed-notifications] and [I-D.ietf-netconf-yang-push] which have been submitted to IESG for publication could be leveraged for an HTTP-based subscription for EPCP. Specifically, it could be used for the posture collection manager to continuously receive posture changes as they happen from the posture collection engine. At this point, it seems like [I-D.ietf-netconf-restconf-notif] would be a good match to these requirements. However further investigation into the applicability of supporting a RESTCONF server capability on to handle subscription requests needs to be made. Specific questions which should be examined include:
* Number of endpoints which can be continuously tracked by a single posture collection manager. Scalability questions to be considered include elements from the number of transport connects maintained to the volume of volume and churn of posture evidence which will be continuously pushed to the posture collection manager manager.

* Ability of the posture collection manager to establish and maintain a continuous state of endpoint posture during failures. This includes failures/reboots on either side of the interface.

* Ability to support for the full set of functions described for NETCONF within Section 5.

  o Add support endpoint types beyond workstations, servers, and network infrastructure devices.

  o Examine the integration of [I-D.ietf-mile-xmpp-grid].

  o Define a standard interface and API for interacting with the repository. Requirements to consider include: creating a secure channel between a publisher and the repository, creating a secure channel between a subscriber and the repository, and the types of interactions that must be supported between publishers and subscribers to a repository.

  o Define a standard interface for communications between the posture broker client and posture transport client(s) as well as the posture broker server and posture transport server(s).

  o Retention of posture information on the target endpoint.

  o Define an orchestrator component as well as publish/subscribe interface for it.

  o Define an evaluator component as well as an interface for it.

  o Reassess the use of MAC addresses, including market research to determine if MAC addresses continue to be a widely implemented device identifier among network tools.

7. Acknowledgements

The authors wish to thank all of those in the TCG TNC work group who contributed to development of the TNC ECP specification upon which this document is based.

<table>
<thead>
<tr>
<th>Member</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Padma Krishnaswamy</td>
<td>Battelle Memorial Institute</td>
</tr>
<tr>
<td>Eric Fleischman</td>
<td>Boeing</td>
</tr>
<tr>
<td>Richard Hill</td>
<td>Boeing</td>
</tr>
<tr>
<td>Steven Venema</td>
<td>Boeing</td>
</tr>
<tr>
<td>Nancy Cam-Winget</td>
<td>Cisco Systems</td>
</tr>
<tr>
<td>Scott Pope</td>
<td>Cisco Systems</td>
</tr>
<tr>
<td>Max Pritikin</td>
<td>Cisco Systems</td>
</tr>
<tr>
<td>Allan Thompson</td>
<td>Cisco Systems</td>
</tr>
<tr>
<td>Nicolai Kuntze</td>
<td>Fraunhofer Institute for Secure Information Technology (SIT)</td>
</tr>
<tr>
<td>Ira McDonald</td>
<td>High North</td>
</tr>
<tr>
<td>Dr. Andreas Steffen</td>
<td>HSR University of Applied Sciences</td>
</tr>
<tr>
<td></td>
<td>Rapperswil</td>
</tr>
<tr>
<td>Josef von Helden</td>
<td>Hochschule Hannover</td>
</tr>
<tr>
<td>James Tan</td>
<td>Infoblox</td>
</tr>
<tr>
<td>Steve Hanna (TNC-WG Co-Chair)</td>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Cliff Kahn</td>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Lisa Lorenzin</td>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Atul Shah (TNC-WG Co-Chair)</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Jon Baker</td>
<td>MITRE</td>
</tr>
<tr>
<td>Charles Schmidt</td>
<td>MITRE</td>
</tr>
<tr>
<td>Rainer Enders</td>
<td>NCP Engineering</td>
</tr>
<tr>
<td>Dick Wilkins</td>
<td>Phoenix Technologies</td>
</tr>
</tbody>
</table>
Table 1: Members of the TNC Work Group that Contributed to the Document

Special thanks also to Dan Ehrlich, Kathleen Moriarty, David Oliva and Eric Voit for their thoughtful comments and edits.

8. IANA Considerations

This document does not define any new IANA registries. However, this document does reference other documents that do define IANA registries. As a result, the IANA Considerations section of the referenced documents should be consulted.

9. Security Considerations

This Security Considerations section includes an analysis of the attacks that may be mounted against systems that implement the EPCP (Section 9.1) and the countermeasures that may be used to prevent or mitigate these attacks (Section 9.2). Overall, a substantial reduction in cyber risk can be achieved.

9.1. Threat Model

This section lists the attacks that can be mounted on a NEA implementation of an EPCP environment. The following section (Section 9.2) describes countermeasures.

Because the EPCP describes a specific use case for NEA components, many security considerations for these components are addressed in more detail in the technical specifications: [RFC8412], [IF-IMC], [RFC5793], [Server-Discovery], [RFC6876], [IF-IMV].
9.1.1. Endpoint Attacks

While the EPCP provides substantial improvements in endpoint security, endpoints can still be compromised. For this reason, all parties must regard data coming from endpoints as potentially unreliable or even malicious. An analogy can be drawn with human testimony in an investigation or trial. Human testimony is essential but must be regarded with suspicion.

- Compromise of endpoint: A compromised endpoint may report false information to confuse or even provide maliciously crafted information with a goal of infecting others.

- Putting bad information in SWID directory: Even if an endpoint is not completely compromised, some of the software running on it may be unreliable or even malicious. This software, potentially including the SWID generation or discovery tool, or malicious software pretending to be a SWID generation or discovery tool, can place incorrect or maliciously crafted information into the SWID directory. Endpoint users may even place such information in the directory, whether motivated by curiosity or confusion or a desire to bypass restrictions on their use of the endpoint.

- Identity spoofing (impersonation): A compromised endpoint may attempt to impersonate another endpoint to gain its privileges or to besmirch the reputation of that other endpoint. This is of particular concern when using MAC addresses to identify endpoints, which, while widely used in endpoint behavior monitoring and threat assessment tools, are easy to spoof.

9.1.2. Network Attacks

Generally, the network cannot be trusted. A variety of attacks can be mounted using the network, including:

- Eavesdropping, modification, injection, replay, deletion;

- Traffic analysis; and

- Denial of service and blocking traffic.

9.1.3. Posture Manager Attacks

The posture manager is a critical security element and therefore merits considerable scrutiny. A variety of attacks can be leveraged against the Posture Manager.
Compromised trusted manager: A compromised posture manager or a malicious party that is able to impersonate a posture manager can incorrectly grant or deny access to endpoints, place incorrect information into the repository, or send malicious messages to endpoints.

Misconfiguration of posture manager: Accidental or purposeful misconfiguration of a trusted posture manager can cause effects that are similar to those listed for compromised trusted posture manager.

Malicious untrusted posture manager: An untrusted posture manager cannot mount any significant attacks because all properly implemented endpoints will refuse to engage in any meaningful dialog with such a posture manager.

9.1.4. Repository Attacks

The repository is also an important security element and therefore merits careful scrutiny.

Putting bad information into trusted repository: An authorized repository client such as a server may be able to put incorrect information into a trusted repository or delete or modify historical information, causing incorrect decisions about endpoint security. Placing maliciously crafted data in the repository could even lead to compromise of repository clients, if they fail to carefully check such data.

Compromised trusted repository: A compromised trusted repository or a malicious untrusted repository that is able to impersonate a trusted repository can lead to effects similar to those listed for "Putting bad information into trusted repository". Further, a compromised trusted repository can report different results to different repository clients or deny access to the repository for selected repository clients.

Misconfiguration of trusted repository: Accidental or purposeful misconfiguration of a trusted repository can deny access to the repository or result in loss of historical data.

Malicious untrusted repository: An untrusted repository cannot mount any significant attacks because all properly implemented repository clients will refuse to engage in any meaningful dialog with such a repository.
9.2. Countermeasures

This section lists the countermeasures that can be used in a NEA implementation of an EPCP environment.

9.2.1. Countermeasures for Endpoint Attacks

This profile is in and of itself a countermeasure for a compromised endpoint. A primary defense for an endpoint is to run up to date software configured to be run as safely as possible.

Ensuring that anti-virus signatures are up to date and that a firewall is configured are also protections for an endpoint that are supported by the current NEA specifications.

For secure device identification and to correlate device identifiers if the MAC address is randomized, MAC addresses should be collected along with other, more secure endpoint identifiers. Endpoints that have hardware cryptographic modules that are provisioned by the enterprise, in accordance with [IEEE-802-1ar], can protect the private keys used for authentication and help prevent adversaries from stealing credentials that can be used for impersonation. Future versions of the EPCP may want to discuss in greater detail how to use a hardware cryptographic module, in accordance with [IEEE-802-1ar], to protect credentials and to protect the integrity of the code that executes during the bootstrap process by hashing or recording indicators of compromise.

9.2.2. Countermeasures for Network Attacks

To address network attacks, [RFC6876] includes required encryption, authentication, integrity protection, and replay protection. [Server-Discovery] also includes authorization checks to ensure that only authorized servers are trusted by endpoints. Any unspecified or not yet specified network protocols employed in the EPCP (e.g. the protocol used to interface with the repository) should include similar protections.

These protections reduce the scope of the network threat to traffic analysis and denial of service. Countermeasures for traffic analysis (e.g. masking) are usually impractical but may be employed. Countermeasures for denial of service (e.g. detecting and blocking particular sources) SHOULD be used when appropriate to detect and block denial of service attacks. These are routine practices in network security.
9.2.3. Countermeasures for Posture Manager Attacks

Because of the serious consequences of posture manager compromise, posture managers SHOULD be especially well hardened against attack and minimized to reduce their attack surface. They SHOULD be monitored using the NEA protocols to ensure the integrity of the behavior and analysis data stored on the posture manager and SHOULD utilize an [IEEE-802-1ar]-compliant hardware cryptographic module for identity and/or integrity measurements of the posture manager. They should be well managed to minimize vulnerabilities in the underlying platform and in systems upon which the posture manager depends. Network security measures such as firewalls or intrusion detection systems may be used to monitor and limit traffic to and from the posture manager. Personnel with administrative access to the posture manager should be carefully screened and monitored to detect problems as soon as possible. Posture manager administrators should not use password-based authentication but should instead use non-reusable credentials and multi-factor authentication (where available). Physical security measures should be employed to prevent physical attacks on posture managers.

To ease detection of posture manager compromise, should it occur, posture manager behavior should be monitored to detect unusual behavior (such as a server reboot, unusual traffic patterns, or other odd behavior). Endpoints should log and/or notify users and/or administrators when peculiar posture manager behavior is detected. To aid forensic investigation, permanent read-only audit logs of security-relevant information pertaining to posture manager (especially administrative actions) should be maintained. If posture manager compromise is detected, the posture manager’s certificate should be revoked and careful analysis should be performed of the source and impact of this compromise. Any reusable credentials that may have been compromised should be reissued.

Endpoints can reduce the threat of server compromise by minimizing the number of trusted posture managers, using the mechanisms described in [Server-Discovery].

9.2.4. Countermeasures for Repository Attacks

If the host for the repository is located on its own endpoint, it should be protected with the same measures taken to protect the posture manager. In this circumstance, all messages between the posture manager and repository should be protected with a mature security protocol such as TLS or IPsec.

The repository can aid in the detection of compromised endpoints if an adversary cannot tamper with its contents. For instance, if an
endpoint reports that it does not have an application with a known vulnerability installed, an administrator can check whether the endpoint might be lying by querying the repository for the history of what applications were installed on the endpoint.

To help prevent tampering with the information in the repository:

1. Only authorized parties should have privilege to run code on the endpoint and to change the repository.

2. If a separate endpoint hosts the repository, then the functionality of that endpoint should be limited to hosting the repository. The firewall on the repository should only allow access to the posture manager and to any endpoint authorized for administration.

3. The repository should ideally use "write once" media to archive the history of what was placed in the repository, to include a snapshot of the current status of applications on endpoints.

10. Privacy Considerations

The EPCP specifically addresses the collection of posture data from enterprise endpoints by an enterprise network. As such, privacy is not going to often arise as a concern for those deploying this solution.

A possible exception may be the concerns a user may have when attempting to connect a personal endpoint (such as a phone or mobile endpoint) to an enterprise network. The user may not want to share certain details, such as an endpoint identifier or SWID tags, with the enterprise. The user can configure their NEA client to reject requests for this information; however, it is possible that the enterprise policy will not allow the user’s endpoint to connect to the network without providing the requested data.

An enterprise network should limit access to endpoint posture and identification information to authorized users.

11. References

11.1. Informative References

11.2. Normative References

[I-D.ietf-mile-xmpp-grid]

[I-D.ietf-netconf-restconf-notif]

[I-D.ietf-netconf-subscribed-notifications]

[I-D.ietf-netconf-yang-push]
[I-D.ietf-sacm-terminology]


Appendix A.  Rationale for an EPCP Solution

A.1.  Preventative Posture Assessments

The value of continuous endpoint posture assessment is well established. Security experts have identified asset management and vulnerability remediation as a critical step for preventing intrusions. Application whitelisting, patching applications and operating systems, and using the latest versions of applications top the Defense Signals Directorate's "Top 4 Mitigations to Protect Your ICT System". [DSD] "Inventory of Authorized and Unauthorized Endpoints", "Inventory of Authorized and Unauthorized Software", and "Continuous Vulnerability Assessment and Remediation" are Controls 1, 2, and 3, respectively, of the CIS Controls [CIS]. While there are commercially available solutions that attempt to address these security controls, these solutions do not run on all types of endpoints; consistently interoperate with other tools that could make use of the data collected; collect posture information from all types of endpoints in a consistent, standardized schema; or require vetted,
standardized protocols that have been evaluated by the international community for cryptographic soundness.

As is true of most solutions offered today, the solution found in the EPCP does not attempt to solve the lying endpoint problem, or detect infected endpoints; rather, it focuses on ensuring that healthy endpoints remain healthy by keeping software up-to-date and patched.

A.2. All Network-Connected Endpoints areEndpoints

As defined by [I-D.ietf-sacm-terminology], an endpoint is any physical or virtual computing endpoint that can be connected to a network. Posture assessment against policy is equally, if not more, important for continuously connected endpoints, such as enterprise workstations and infrastructure endpoints, as it is for sporadically connected endpoints. Continuously connected endpoints are just as likely to fall out of compliance with policy, and a standardized posture assessment method is necessary to ensure they can be properly handled.

A.3. All Endpoints on the Network Must be Uniquely Identified

Many administrators struggle to identify what endpoints are connected to the network at any given time. By requiring a standardized method of endpoint identity, the EPCP will enable administrators to answer the basic question, "What is on my network?" In [I-D.ietf-sacm-terminology], SACM defines this set of endpoints on the network as the SACM domain. Unique endpoint identification also enables the comparison of current and past endpoint posture assessments, by allowing administrators to correlate assessments from the same endpoint. This makes it easier to flag suspicious changes in endpoint posture for manual or automatic review, and helps to swiftly identify malicious changes to endpoint applications.

A.4. Standardized Data Models

Meeting EPCP best practices requires the use of standardized data models for the exchange of posture information. This helps to ensure that the posture information sent from endpoints to the repository can be easily stored, due to their known format, and shared with authorized endpoints and users.

Posture information must be sent over standardized protocols to ensure the confidentiality and authenticity of this data while in transit. Implementations of the EPCP include [RFC6076] and [RFC6241] for communication between the target endpoint and the posture manager. These protocols allow networks that implement this solution to collect large amounts of posture information from an endpoint.
make decisions about that endpoint’s compliance with some policy. The EPCP offers a solution for all endpoints already connected to the network. Periodic assessments and automated reporting of changes to endpoint posture allow for instantaneous identification of connected endpoints that are no longer compliant to some policy.

A.5. Posture Information Must Be Stored

Posture information must be stored by the repository and must be exposed to an interface at the posture manager. Standard data models enable standard queries from an interface exposed to an administrator at the posture manager console. A repository must retain any current posture information retrieved from the target endpoint and store it indexed by the unique identifier for the endpoint. Any posture collection manager specified by this profile must be able to ascertain from its corresponding posture collection engine whether the posture information is up to date. An interface on the posture manager must support a request to obtain up-to-date information when an endpoint is connected. This interface must also support the ability to make a standard set of queries about the posture information stored by the repository. In the future, some forms of posture information might be retained at the endpoint. The interface on the posture manager must accommodate the ability to make a request to the corresponding posture collection engine about the posture of the target endpoint. Standard data models and protocols also enable the security of posture assessment results. By storing these results indexed under the endpoint’s unique identification, secure storage itself enables endpoint posture information correlation, and ensures that the enterprise’s repositories always offer the freshest, most up-to-date view of the enterprise’s endpoint posture information possible.

A.6. Posture Information Can Be Shared

By exposing posture information using a standard interface and API, other security and operational components have a high level of insight into the enterprise’s endpoints and the software installed on them. This will support innovation in the areas of asset management, vulnerability scanning, and administrative interfaces, as any authorized infrastructure endpoint can interact with the posture information.

A.7. Enterprise Asset Posture Information Belongs to the Enterprise

Owners and administrators must have complete control of posture information, policy, and endpoint mitigation. Standardized data models, protocols and interfaces help to ensure that this posture information is not locked in proprietary databases, but is made available to the enterprise’s repositories.
available to its owners. This enables administrators to develop as nuanced a policy as necessary to keep their networks secure. Of course, there may be exceptions to this such as the case with privacy-related information (e.g., personally identifiable information).

Appendix B. EPCP Supported Use Cases and Non-Supported Use Cases

B.1. Supported Use Cases

The following sections describe the different use cases supported by the EPCP.

B.1.1. Hardware Asset Management

Using the administrative interface on the posture manager, an authorized user can learn:

- what endpoints are connected to the network at any given time; and
- what SWID tags were reported for the endpoints.

The ability to answer these questions offers a standards-based approach to asset management, which is a vital part of enterprise processes such as compliance report generation for the Federal Information Security Modernization Act (FISMA), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), etc.

B.1.2. Software Asset Management

The administrative interface on the posture manager provides the ability for authorized users and infrastructure to know which software is installed on which endpoints on the enterprise’s network. This allows the enterprise to answer questions about what software is installed to determine if it is licensed or prohibited. This information can also drive other use cases such as:

- vulnerability management: knowing what software is installed supports the ability to determine which endpoints contain vulnerable software and need to be patched.
- configuration management: knowing which security controls need to be applied to harden installed software and better protect endpoints.
B.1.3. Vulnerability Management

The administrative interface also provides the ability for authorized users or infrastructure to locate endpoints running software for which vulnerabilities have been announced. Because of

1. the unique IDs assigned to each endpoint; and

2. the rich application data provided in the endpoints’ posture information,

the repository can be queried to find all endpoints running a vulnerable application. Endpoints suspected of being vulnerable can be addressed by the administrator or flagged for further scrutiny.

B.1.4. Threat Detection and Analysis

The repository’s standardized API allows authorized infrastructure endpoints and software to search endpoint posture assessment information for evidence that an endpoint’s software inventory has changed, and can make endpoint software inventory data available to other endpoints. This automates security data sharing in a way that expedites the correlation of relevant network data, allowing administrators and infrastructure endpoints to identify odd endpoint behavior and configuration using secure, standards-based data models and protocols.

B.2. Non-Supported Use Cases

Several use cases, including but not limited to these, are not covered by the EPCP:

o Gathering non-standardized types of posture information: The EPCP does not prevent administrators from collecting posture information in proprietary formats from the endpoint; however it does not set requirements for doing so.

o Solving the lying endpoint problem: The EPCP does not address the lying endpoint problem; the Profile makes no assertions that it can catch an endpoint that is, either maliciously or accidentally, reporting false posture information to the posture manager. However, other solutions may be able to use the posture information collected using the capabilities described in this profile to catch an endpoint in a lie. For example, a sensor may be able to compare the posture information it has collected on an endpoint’s activity on the network to what the endpoint reported to the server and flag discrepancies. However, these capabilities are not described in this profile.
Appendix C. Endpoint Posture Collection Profile Examples

The following subsections provide examples of the EPCP as implemented using components from the NEA architecture.

C.1. Continuous Posture Assessment of an Endpoint

A new application is installed on the endpoint, and the SWID directory is updated. This triggers an update from the SWID posture collector to the SWID posture validator. The message is sent down the NEA stack, encapsulated by NEA protocols until it is sent by the posture transport client to the posture transport server. The posture transport server then forwards it up through the stack, where the layers of encapsulation are removed until the SWID Message arrives at the SWID posture validator.
The SWID posture validator stores the new tag information in the repository. If the tag indicates that the endpoint is compliant to the policy, then the process is complete until the next time an update is needed (either because policy states that the endpoint must submit posture assessment results periodically or because an install/uninstall/update on the endpoint triggers a posture assessment).
If the endpoint has fallen out of compliance with a policy, the posture manager can alert the administrator via the posture manager’s administrative interface. The administrator can then take steps to address the problem. If the administrator has already established a policy for automatically addressing this problem, that policy will be followed.
C.2. Administrator Searches for Vulnerable Endpoints

An announcement is made that a particular version of a piece of software has a vulnerability. The administrator uses the administrative interface on the server to search the repository for endpoints that reported the SWID tag for the vulnerable software.
Figure 8: Admin Searches for Vulnerable Endpoints

The repository returns a list of entries in the matching the administrator’s search. The administrator can then address the vulnerable endpoints by taking some follow-up action such as removing it from the network, quarantining it, or updating the vulnerable software.

Appendix D. Change Log

D.1. -04 to -05

Updated the diagram so the Evaluator and Repository are "current work".

Clarified how the Posture Collection Engine can push data, respond to queries, and establish secure transport connectivity for fulfilling subscriptions.

Expanded on the future work around leveraging NETCONF, RESTCONF, and YANG Push for network devices.
Documented the need to reassess MAC addresses as a device identifier.

Made various typographical and editorial changes.

D.2. -03 to -04

Addressed various comments from the SACM WG.

Refactored the document to better focus it on the communications between endpoints and the posture manager and the best practices for EPCP implementations.

Made other editorial changes and improved consistency throughout the document.

D.3. -02 to -03

Addressed various comments from the SACM WG.

Added a reference to TCG ECP 1.0.

Removed text in the "SWID Posture Validator" section that states it performs evaluation. This was removed because it contradicts the posture manager not performing any evaluations.

Expanded the "Provisioning" section of the "EPCP Transactions" section to include examples of endpoint identifiers and the need to provision endpoints with components and data models.

Combined text for the capabilities of the Administrative Interface and API.

Removed superfluous and introductory text from the "Security Considerations" section.

Renamed section "Vulnerability Searches" to Vulnerability Management".

Changed I-D category to BCP.

Changed references to the NETMOD architecture to the NETCONF architecture because NETCONF represents the management protocol whereas NETMOD is focused on the definition of data models.

Addressed various editorial suggestions.
D.4. -01 to -02

Addressed various comments from the SACM WG.

Added a section for the collection of posture information from network devices using standards from the NETMOD WG.

Updated EPCP component diagrams so they were not specific to a NEA-based implementation.

Updated EPCP NEA example diagrams to reflect all the components in the NEA architecture.

D.5. -00 to -01

There are no textual changes associated with this revision. This revision simply reflects a resubmission of the document so that it remains in active status.

D.6. -01 to -02

Added references to the Software Inventory Message and Attributes (SWIMA) for PA-TNC I-D.

Replaced references to PC-TNC with IF-IMC.

Removed erroneous hyphens from a couple of section titles.

Made a few minor editorial changes.

D.7. -02 to -00

Draft adopted by IETF SACM WG.

D.8. -00 to -01

Significant edits to up-level the draft to describe SACM collection over multiple different protocols.

Replaced references to SANS with CIS.

Made other minor editorial changes.

Authors’ Addresses

Haynes, et al. Expires December 23, 2019
Abstract

This document uses the "information-type" extension point as defined in the Resource-Oriented Lightweight Information Exchange (ROLIE) [RFC8322] Section 7.1.2 to better support Software Record and Software Inventory use cases. This specification registers a new ROLIE information-type, "software-descriptor", that allows for the categorization of information relevant to software description activities and formats. In particular, the usage of the ISO 19770-2:2015 (SWID Tag) and the Concise SWID (COSWID) formats in ROLIE are standardized. Additionally, this document discusses requirements and usage of other ROLIE elements in order to best syndicate software description information.
1. Introduction

This document defines an extension to the Resource-Oriented Lightweight Information Exchange (ROLIE) [RFC8322] to support the publication of software descriptor information. Software descriptor information is information that characterizes static software components, packages, and installers; including identifying, versioning, software creation and publication, and file artifact information.

Software descriptor information provides data about what might be installed, but doesn’t describe a specific software installation’s
configuration or execution. This static approach to software description is a smaller state space that covers the majority of current use cases for software inventory and record keeping.

Some possible use cases for software descriptor information ROLIE Feeds include:

- Software providers can publish software descriptor information so that software researchers, enterprises, and users of software can understand the collection of software produced by that software provider.

- Organizations can aggregate and syndicate collections of software descriptor information provided by multiple software providers to support software-related analysis processes (e.g., vulnerability analysis) and value added information (e.g., software configuration checklist repository) using identification and characterization information derived from software descriptor information.

- End user organizations can consume sources of software descriptor information, and other related software vulnerability and configuration information to provide the data needed to automate software asset, patch, and configuration management practices.

- Organizations can use software descriptors to support verification of other entities, thru mechanisms such as RIM or other integrity measurements.

This document supports these use cases by describing the content requirements for Feeds and Entries of software descriptor information that are to be published to or retrieved from a ROLIE repository.

2. Terminology

The key words "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Several places in this document refer to the "information-type" of a Resource (Entry or Feed). This refers to the "value" attribute of an "atom:category" element whose scheme is "urn:ietf:params:rolie:category:information-type". For an Entry, this value can be inherited from it's containing Feed as per [RFC8322].
3. Background

In order to effectively protect and secure an endpoint, it is vital to know what the software load of that endpoint is. This software load, the combination of software, patches and installers on a device, represents the majority of the endpoint’s attack surface. Unfortunately, without a reliable and secure package manager, or otherwise a secured and managed operating system, tracking what software is installed on an endpoint is currently not feasible without undue effort. Even attempting to whitelist software is difficult without a way of identifying software and its editions, versions and hotfixes.

Software descriptor information, such as that standardized in the ISO 19770-2:2015 SWID Tag format, or expressed in proprietary enterprise databases, attempts to provide as much data about this software as possible.

Once this information is expressed, it needs to be stored and shared to internal and external parties. ROLIE provides a mechanism to handle this sharing in an automation-friendly way.

4. The "software-descriptor" information type

When an "atom:category" element has a "scheme" attribute equal to "urn:ietf:params:rolie:category:information-type", the "term" attribute defines the information type of the associated resource. A new information type value: "software-descriptor", is described in this section, and registered in Section 8.1.

The "software-descriptor" information type represents any static information that describes a piece of software. This document uses the definition of software provided by [RFC4949]. Note that as per this definition, this information type pertains to static software, that is, code on the disc. The "software-descriptor" information type is intended to provide a category for information that does one or more of the following:

identifies and characterizes software: This software identification and characterization information can be provided by a large variety of data, but always describes software in a pre-installed state.

provides software installer metadata: This represents information about software used to install other software. This metadata identifies, and characterizes a software installation package or media.
describes stateless installation metadata: Information that describes the software post-deployment, such as files that may be deployed during an installation. It is expected that this metadata is produced generally for a given installation, and may not exactly match the actual installed files on a given endpoint.

Provided below is a non-exhaustive list of information that may be considered to be of a software-descriptor information type.

- **Naming information**: IDs and names that aid in the identification of a piece of software
- **Version and patching information**: Version numbers, patch identifiers, or other information that
- **Vendor and source information**: Includes where the software was developed or distributed from, as well as where the software installation media may be located.
- **Payload and file information**: Information that describes or enumerates the files and folders that make up the piece of software, and information about those files.
- **Descriptive information and data**: Any information that otherwise characterizes a piece of software, such as libraries, runtime environments, target OSes, intended purpose or audience, etc.

Note again that this list is not exhaustive, any information that in is the abstract realm of an incident should be classified under this information-type.

It is important to note that software descriptor information is static for a given piece of software. That is, the information expressed is the data that doesn’t change from the publication of the software to its final install. Information about the current status (e.g. install location, memory usage, CPU usage, launch parameters, job progress, etc.), is out of scope of this information type.

5. **rolie:property Extensions**

This document registers new valid rolie:property names as follows:

5.1. **urn:ietf:params:rolie:property:swd:swname**

This property provides an exposure point for the plain text name of the software being described. Naming of software is not a well standardized process, and software names can change between product versions or editions. As such, care should be taken that this value
is set as consistently as possible by generating it directly from an attached software descriptor resource.

5.2. urn:ietf:params:rolie:property:swd:swversion

This property provides an exposure point for the version of the software being described. This value should be generated or taken from the software descriptor linked to by the entry. This helps avoid, but does not prevent, inconsistent versioning schemes being shared.

5.3. urn:ietf:params:rolie:property:swd:swcreator

This property provides an exposure point for a plain text name of the creator of the software being described. This is in many cases an organization or company, but certainly could be a single person. Most software descriptor formats include this information, and where possible, this property should be set equal to that value.

6. Data format requirements

This section defines usage guidance and additional requirements related to data formats above and beyond those specified in [RFC8322]. The following formats are expected to be commonly used to express software descriptor information. For this reason, this document specifies additional requirements to ensure interoperability.

6.1. The ISO SWID 2015 format

6.1.1. Description

ISO/IEC 19770-2:2015 defines a software record data format referred to as a "SWID Tag". It provides several tag types:

- primary: provides descriptive and naming information about software,
- patch: describes non-standalone software meant to patch existing software,
- corpus: describes the software installation media that installs a given piece of software,
- supplemental: provides additional metadata to be deployed alongside a tag.
For a more complete overview as well as normative requirements, refer to ISO/IEC 19770-2:2015 [SWID].

For additional requirements and guidance around creation of SWID Tags, consult NIST Internal Report 8060 [NISTIR8060].

6.1.2. Requirements

For an Entry to be considered as a "SWID Tag Entry", it MUST fulfill the following conditions:

- The information-type of the Entry is "software-descriptor". For a typical Entry, this is derived from the information type of the Feed it is contained in. For a standalone Entry, this is provided by an "atom:category" element.

- The document linked to by the "href" attribute of the "atom:content" element is a 2015 SWID Tag as per ISO/IEC 19770-2:2015.

A "SWID Tag Entry" MUST conform to the following requirements:

- The value of the "type" attribute of the "atom:content" element MUST be "application/xml".

- There MUST be one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:content-id" and the "value" attribute exactly equal to the "<tagid>" element in the attached SWID Tag. This allows for ROLIE consumers to more easily search for SWID tags without needing to download the tag itself.

- There MUST be one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:swd:swname", and the "value" attribute equal to the value of the "<name>" element in the attached SWID Tag. As above, this field aids ROLIE consumers in search and filtering Entries.

- There MAY be a property element with the "name" attribute equal to "urn:ietf:params:rolie:property:swd:swversion". When this property appears, its value MUST be equal to the value of the "version" element in the attached SWID Tag.

6.2. The Concise SWID format
6.2.1. Description

The Concise SWID (COSWID) format is an alternative representation of the SWID Tag format using a Concise Binary Object Representation (CBOR) encoding. This provides the format with a reduced size that is more suitable for constrained devices. It provides the same features and attributes as are specified in ISO 19770-2:2015, plus:

- a straightforward method to sign and encrypt using COSE, and
- additional attributes that provide an improved structure to include file hashes intended to be used as Reference Integrity Measurements (RIM).

For more information and the complete specification, refer to the COSWID internet draft [I-D.ietf-sacm-coswid].

6.2.2. Requirements

For an Entry to be considered as a "COSWID Tag Entry", it MUST fulfill the following conditions:

- The information-type of the Entry is "software-descriptor". For a typical Entry, this is derived from the information-type of the Feed it is contained in. For a standalone Entry, this is provided by an "atom:category" element.

- The document linked to by the "href" attribute of the "atom:content" element is a COSWID Tag as per [I-D.ietf-sacm-coswid]

A "COSWID Tag Entry" MUST conform to the following requirements:

- The value of the "type" attribute of the atom:content element MUST be "application/coswid+cbor".

- There MUST be one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:content-id" and the "value" attribute exactly equal to the "tag-id" element in the attached COSWID Tag (mapped to integer 0). This allows for ROLIE consumers to more easily search for COSWID tags without needing to download the tag itself.

- There MUST be one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:swd:swname", and the "value" attribute equal to the value of the "swid-name" element in the attached COSWID Tag (mapped to the integer 1). As above, this field aids ROLIE consumers in searching and filtering Entries.
There MAY be a property element with the "name" attribute equal to "urn:ietf:params:rolie:property:swd:swversion". When this property appears, its value MUST be equal to the value of the tag-version element in the attached COSWID Tag (mapped to the integer 12).

7. atom:link Extensions

This section defines additional link relationships that implementations MUST support. These relationships are not registered in the Link Relation IANA table as their use case is too narrow. Each relationship is named and described.

These relations come in related pairs. The first of each pair is expected to be more common, as they can be determined at the time that the Entry is created. The second of each pair will often need to be added retroactively to an Entry.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ancestor</td>
<td>Links to a software descriptor resource that defines an ancestor of the</td>
</tr>
<tr>
<td></td>
<td>software being described by this Entry. This is usually a previous version</td>
</tr>
<tr>
<td>descendent</td>
<td>Links to a software descriptor resource that defines a descendent of the</td>
</tr>
<tr>
<td></td>
<td>software being described by this Entry. This is usually a more recent</td>
</tr>
<tr>
<td></td>
<td>version or edition of the software.</td>
</tr>
<tr>
<td>patches</td>
<td>Links to a software descriptor resource that defines the software being</td>
</tr>
<tr>
<td>patchedby</td>
<td>Links to a software descriptor resource that defines the patch or update</td>
</tr>
<tr>
<td>requires</td>
<td>Links to a software descriptor resource that defines a piece of software</td>
</tr>
<tr>
<td>requiredBy</td>
<td>Links to a software descriptor resource that defines a piece of software</td>
</tr>
<tr>
<td>installs</td>
<td>Links to a software descriptor resource that defines the software that is</td>
</tr>
<tr>
<td>installedBy</td>
<td>Links to a software descriptor resource that defines the software package</td>
</tr>
<tr>
<td>patchesVulnerability</td>
<td>Links to a vulnerability that this software update fixes. Used for software</td>
</tr>
<tr>
<td>hasVulnerability</td>
<td>Links to a vulnerability description object that details a vulnerability</td>
</tr>
</tbody>
</table>

Table 1: Link Relations for Resource-Oriented Lightweight Indicator Exchange
8. IANA Considerations

8.1. software-descriptor information-type

IANA has added an entry to the "ROLIE Security Resource Information Type Sub-Registry" registry located at <https://www.iana.org/assignments/rolie/category/information-type>.

The entry is as follows:

   name: software-descriptor
   index: TBD
   reference: This document, Section 4

8.2. swd:swname property

IANA has added an entry to the "ROLIE URN Parameters" registry located in <https://www.iana.org/assignments/rolie/>.

The entry is as follows:

   name: property:swd:swname
   Reference: This document, Section 5.1
   Subregistry: None

8.3. swd:swversion property

IANA has added an entry to the "ROLIE URN Parameters" registry located in <https://www.iana.org/assignments/rolie/>.

The entry is as follows:

   name: property:swd:swversion
   Reference: This document, Section 5.1
   Subregistry: None
8.4. swd:swcreator property

IANA has added an entry to the "ROLIE URN Parameters" registry located in <https://www.iana.org/assignments/rolie/>.

The entry is as follows:

name: property:swd:swcreator


Reference: This document, Section 5.1

Subregistry: None

9. Security Considerations

Use of this extension implies dealing with the security implications of both ROLIE and of software descriptors in general. As with any data, care should be taken to verify the trustworthiness and veracity of the descriptor information to the fullest extent possible.

Ideally, software descriptors should have been signed by the software manufacturer, or signed by whichever agent processed the source code. Software descriptor documents from these sources are more likely to be accurate than those generated by scraping installed software.

These "authoritative" sources of software descriptor content should consider additional security for their ROLIE repository beyond the typical recommendations, as the central importance of the repository is likely to make it a target.

Version information is often represented differently across manufacturers and even across product releases. If using software version information for low fault tolerance comparisons and searches, care should be taken that the correct version scheme is being utilized.

10. Normative References

[I-D.ietf-sacm-coswid]
Appendix A. Schema

This document does not require any schema extensions.

Appendix B. Examples of Use

Use of this extension in a ROLIE repository will not typically change that repository’s operation. As such, the general examples provided by the ROLIE core document would serve as examples. Provided below is a sample software descriptor ROLIE entry:

Banghart & Waltermire  Expires September 28, 2019  [Page 13]
<xml version="1.0" encoding="UTF-8"/>
<entry xmlns="http://www.w3.org/2005/Atom"
    xmlns:rolie="urn:ietf:params:xml:ns:rolie-1.0">
    <id>dd786dba-88e6-440b-9158-b8fae67ef67c</id>
    <title>Sample Software Descriptor</title>
    <published>2015-08-04T18:13:51.0Z</published>
    <updated>2015-08-05T18:13:51.0Z</updated>
    <summary>A descriptor for a piece of software published by this organization.</summary>
    <link rel="self" href="http://www.example.org/rolie/SWD/123456"/>
    <link rel="feed" href="http://www.example.org/rolie/SWD/"/>
    <link rel="requires" href="http://www.example.org/rolie/SWD/78430"/>
    <rolie:property name="urn:ietf:params:rolie:property:swd:swname" value="Example Software Name"/>
    <category
        scheme="urn:ietf:params:rolie:category:information-type" term="software-descriptor"/>
    <rolie:format
        ns="http://standards.iso.org/iso/19770/-2/2015/schema.xsd"/>
    <content type="application/xml" src="http://www.example.org/rolie/SWD/123456/data"/>
</entry>

Authors' Addresses

Stephen Banghart
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland  20877
USA

Email: stephen.banghart@nist.gov

David Waltermire
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland  20877
USA

Email: david.waltermire@nist.gov
Security Automation and Continuous Monitoring (SACM) Terminology
draft-ietf-sacm-terminology-16

Abstract

This memo documents terminology used in the documents produced by SACM (Security Automation and Continuous Monitoring).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on June 17, 2019.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.  Introduction . . . . . . . . . . . . . . . . . . . . . . . .   2
2.  Terms and Definitions . . . . . . . . . . . . . . . . . . . .   2
3.  IANA Considerations . . . . . . . . . . . . . . . . . . . . .  21
4.  Security Considerations . . . . . . . . . . . . . . . . . . .  21
5.  Acknowledgements . . . . . . . . . . . . . . . . . . . . . .  22
6.  Change Log . . . . . . . . . . . . . . . . . . . . . . . . .  22
7.  Contributors . . . . . . . . . . . . . . . . . . . . . . . . .  26
8.  References . . . . . . . . . . . . . . . . . . . . . . . . . .  27
  8.1.  Normative References . . . . . . . . . . . . . . . . . .  28
  8.2.  Informative References . . . . . . . . . . . . . . . . .  28
Appendix A.  The Attic . . . . . . . . . . . . . . . . . . . . .  29
Authors’ Addresses . . . . . . . . . . . . . . . . . . . . . . .  29

1.  Introduction

Our goal with this document is to improve our agreement on the terminology used in documents produced by the IETF Working Group for Security Automation and Continuous Monitoring. Agreeing on terminology should help reach consensus on which problems we’re trying to solve, and propose solutions and decide which ones to use.

2.  Terms and Definitions

This section describes terms that have been defined by other RFC’s and defines new ones. The predefined terms will reference the RFC and where appropriate will be annotated with the specific context by which the term is used in SACM. Note that explanatory or informational augmentation to definitions are segregated from the definitions themselves. The definition for the term immediately follows the term on the same line, whereas expositional text is contained in subsequent paragraphs immediately following the definition.

Assertion: Defined by the ITU in [X.1252] as "a statement made by an entity without accompanying evidence of its validity".

In the context of SACM, an assertion is the output of a SACM Component in the form of a SACM Statement (including metadata about the data source and data origin, e.g. timestamps). While the validity of an assertion about Content and Content Metadata cannot be verified without, for example, Integrity Proofing of the...
Data Source, an assertion (and therefore a SACM statement, respectively) of the validity of Statement Metadata can by enabled by including corresponding Integrity Evidence created by the Data Origin.

Assessment: Defined in [RFC5209] as "the process of collecting posture for a set of capabilities on the endpoint (e.g., host-based firewall) such that the appropriate validators may evaluate the posture against compliance policy."

Attribute: Is a data element, as defined in [RFC5209], that is atomic.

In the context of SACM, attributes are "atomic" information elements and an equivalent to attribute-value-pairs. Attributes can be components of Subjects, the basic composite definitions that are defined in the SACM Information Model.

Capability: A set of features that are available from a SACM Component.

See also "capability" in [I-D.ietf-i2nsf-terminology].

In the context of SACM, the extent of a SACM component’s ability is enabled by the functions it is composed of. Capabilities are registered at a SACM broker (potentially also at a proxy or a repository component if it includes broker functions) by a SACM component via the SACM component registration task and can be discovered by or negotiated with other SACM components via the corresponding tasks. For example, the capability of a SACM provider may be to provide target endpoint records (declarative guidance about well-known or potential target endpoints), or only a subset of that data.

A capability’s description is in itself imperative guidance on what functions are exposed to other SACM components in a SACM domain and how to use them in workflows.

The SACM Vulnerability Assessment Scenario [I-D.ietf-sacm-vuln-scenario] defines the terms Endpoint Management Capabilities, Vulnerability Management Capabilities, and Vulnerability Assessment Capabilities, which illustrate specific sets of SACM capabilities on an enterprise IT department’s point of view and therefore compose sets of declarative guidance.
Collection Result: Is a composition of one or more content elements carrying information about a target endpoint, that is produced by a collector when conducting a collection task.

Collection Task: A targeted task that collects attributes and/or corresponding attribute values from target endpoint.

There are four types of frequency collection tasks can be conducted with:

- ad-hoc, e.g. triggered by a unsolicited query
- conditional, e.g. triggered in accordance with policies included in the compositions of workflows
- scheduled, e.g. in regular intervals, such as every minute or weekly
- continuously, e.g. a network behavior observation

There are three types of collection methods, each requiring an appropriate set of functions to be included in the SACM component conducting the collection task:

- Self-Reporting: A SACM component located on the target endpoint itself conducts the collection task.
- Remote-Acquisition: A SACM component located on an Endpoint different from the target endpoint conducts the collection task via interfaces available on the target endpoint, e.g. SNMP/NETCONF or WMI.
- Behavior-Observation: A SACM component located on an Endpoint different from the target endpoint observes network traffic related to the target endpoint and conducts the collection task via interpretation of that network traffic.

Collector: A piece of software that acquires information about one or more target endpoints by conducting collection tasks.

A collector can be distributed across multiple endpoints, e.g. across a target endpoint and a SACM component. The separate parts of the collector can communicate with a specialized protocol, such as PA-TNC [RFC5792]. At least one part of a distributed collector has to take on the role of a provider of information by providing SACM interfaces to propagate capabilities and to provide SACM content in the form of collection results.
Configuration: A non-volatile subset of the endpoint attributes of a endpoint that is intended to be unaffected by a normal reboot-cycle.

Configuration is a type of imperative guidance that is stored in files (files dedicated to contain configuration and/ or files that are software components), directly on block devices, or on specific hardware components that can be accessed via corresponding software components. Modification of configuration can be conducted manually or automatically via management (plane) interfaces that support management protocols, such as SNMP or WMI. A change of configuration can occur during both run-time and down-time of an endpoint. It is common practice to scheduled a change of configuration during or directly after the completion of a boot-cycle via corresponding software components located on the target endpoint itself.

Examples: The static association of an IP address and a MAC address in a DHCP server configuration, a directory-path that identifies a log-file directory, a registry entry.

Configuration Drift: The disposition of endpoint characteristics to change over time.

Configuration drift exists for both hardware components and software components. Typically, the frequency and scale of configuration drift of software components is significantly higher than the configuration drift of hardware components.

Consumer: A SACM Role that requires a SACM Component to include SACM Functions enabling it to receive information from other SACM Components.

Content Element: Content elements constitute the payload data (SACM content) transferred via statement Subjects emitted by providers of information. Every content element Subject includes a specific content Subject and a corresponding content metadata Subject.

Content Metadata: Data about content Subjects. Every content-element includes a content metadata Subject. The Subject can include any information element that can annotate the content transferred. Examples include time stamps or data provenance Subjects.

Control Plane: An architectural component that provides common control functions to all SACM components.
Typically used as a term in the context of routing, e.g. [RFC6192]. SACM components may include authentication, authorization, (capability) discovery or negotiation, registration and subscription. The control plane orchestrates the flow on the data plane according to imperative guidance (i.e. configuration) received via the management plane. SACM components with interfaces to the control plane have knowledge of the capabilities of other SACM components within a SACM domain.

Controller: A controller is a SACM Role that is assigned to a SACM component containing control plane functions managing and facilitating information sharing or execute on security functions. There are three types of SACM controllers: Broker, Proxy, and Repository. Depending on its type, a controller can also contain functions that have interfaces on the data plane.

Data Confidentiality: Defined in [RFC4949] as "the property that data is not disclosed to system entities unless they have been authorized to know the data."

Data In Motion: Data that is being transported via a network; also referred to as "Data in Transit" or "Data in Flight".

Data in motion requires a data model to transfer the data using a specific encoding. Typically, data in motion is serialized (marshalling) into a transport encoding by a provider of information and deserialized (unmarshalling) by a consumer of information. The termination points of provider of information and consumer of information data is transferred between are interfaces. In regard to data in motion, the interpretation of the roles consumer of information and provider of information depends on the corresponding OSI layer (e.g. on layer2: between interfaces connected to a broadcast domain, on layer4: between interfaces that maintain a TCP connection). In the context of SACM, consumer of information and provider of information are SACM components.

Data At Rest: Data that is stored.

Data at rest requires a data model to encode the data to be stored. In the context of SACM, data at rest located on a SACM component can be provided to other SACM components via discoverable capabilities.

Data Integrity: Defined in [RFC4949] as "the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner."
Data Origin: The SACM Component that initially acquired or produced data about an endpoint.

Data Origin enables a SACM component to identify the SACM component that initially acquired or produced data about a (target) endpoint (e.g. via collection from a data source) and made it available to a SACM domain via a SACM statement. Data Origin can be expressed by an endpoint label information element (e.g. to be used as metadata in statement).

Data Plane: Is an architectural component providing operational functions enabling information exchange that is not command and control or management related.

Typically used as a term in the context of routing (and used as a synonym for forwarding plane, e.g. [RFC6192]). In the context of SACM, the data plane is an architectural component providing operational functions to enable a SACM component to provide and consume SACM statements and therefore SACM content, which composes the actual SACM content. The data plane in a SACM domain is used to conduct distributed SACM tasks by transporting SACM content via specific transport encodings and corresponding operations defined by SACM data models.

Data Provenance: An historical record of the sources, origins and evolution, as it pertains to data, that is influenced by inputs, entities, functions and processes.

Additional Information - In the context of SACM, data provenance is expressed as metadata that identifies SACM statements and corresponding content elements a new statement is created from. In a downstream process, this references can cascade, creating a data provenance tree that enables SACM components to trace back the original data sources involved in the creation of SACM statements and take into account their characteristics and trustworthiness.

Data Source: Is an endpoint from which a particular set of attributes and/or attribute values have been collected.

Data Source enables a SACM component to identify – and potentially characterize – a (target) endpoint that is claimed to be the original source of endpoint attributes in a SACM statement. Data Source can be expressed as metadata by an endpoint label information element or a corresponding subject of identifying endpoint attributes.
Endpoint: Defined in [RFC5209] as "any computing device that can be connected to a network."

Additional Information - The [RFC5209] definition continues, "Such devices normally are associated with a particular link layer address before joining the network and potentially an IP address once on the network. This includes: laptops, desktops, servers, cell phones, or any device that may have an IP address."

To further clarify the [RFC5209] definition, an endpoint is any physical or virtual device that may have a network address. Note that, network infrastructure devices (e.g. switches, routers, firewalls), which fit the definition, are also considered to be endpoints within this document.

Physical endpoints are always composites that are composed of hardware components and software components. Virtual endpoints are composed entirely of software components and rely on software components that provide functions equivalent to hardware components.

The SACM architecture differentiates two essential categories of endpoints: Endpoints whose security posture is intended to be assessed (target endpoints) and endpoints that are specifically excluded from endpoint posture assessment (excluded endpoints).

Based on the definition of an asset, an endpoint is a type of asset.

Endpoint Attribute: Is a discreet endpoint characteristic that is computably observable.

Endpoint Attributes typically constitute Attributes that can be bundled into Subject (e.g. information about a specific network interface can be represented via a set of multiple AVP).

Endpoint Characteristics: The state, configuration and composition of the software components and (virtual) hardware components a target endpoint is composed of, including observable behavior, e.g. sys-calls, log-files, or PDU emission on a network.

In SACM work-flows, (Target) Endpoint Characteristics are represented via Information Elements.

Endpoint Characterization Task: The task of endpoint characterization that uses endpoint attributes that represent distinct endpoint characteristics.
Endpoint Classification: The categorization of the endpoint into one or more taxonomic structures.

Endpoint classification requires declarative guidance in the form of an endpoint profile, discovery results and potentially collection results. Types, classes or the characteristics of an individual target endpoint are defined via endpoint profiles.

Endpoint Classification Task: The task of endpoint classification that uses an endpoint’s characteristics to determine how to categorize the given endpoint into one or more taxonomic structures.

Endpoint Label: A unique label associated with a unique endpoint.

Endpoint specializations have corresponding endpoint label specializations. For example, an endpoint label used on a SACM Component is a SACM Component Label.

Endpoint Management Capabilities: Enterprise IT management capabilities that are tailored to manage endpoint identity, endpoint information, and associated metadata.

Evaluation Task: A task by which an endpoint’s asserted attribute value is evaluated against a policy-compliant attribute value.

Evaluation Result: The resulting value from having evaluated a set of posture attributes.

Expected Endpoint Attribute State: The policy-compliant state of an endpoint attribute that is to be compared against.

Sets of expected endpoint attribute states are transported as declarative guidance in target endpoint profiles via the management plane. This, for example, can be a policy, but also a recorded past state. An expected state is represented by an Attribute or a Subject that represents a set of multiple attribute value pairs.

Guidance: Machine-processable input directing SACM processes or tasks.

Examples of such processes/tasks include automated device management, remediation, collection, evaluation. Guidance influences the behavior of a SACM Component and is considered content of the management plane. In the context of SACM, guidance is machine-readable and can be manually or automatically generated.
or provided. Typically, the tasks that provide guidance to SACM components have a low-frequency and tend to be sporadic.

There are two types of guidance:

Declarative Guidance: Guidance that defines the configuration or state an endpoint is supposed to be in, without providing specific actions or methods to produce that desired state. Examples include Target Endpoint Profiles or network topology based requirements.

Imperative Guidance: Guidance that prescribes specific actions to be conducted or methods to be used in order to achieve an outcome. Examples include a targeted Collection Task or the IP-Address of a SACM Component that provides a registration function.

Prominent examples include: modification of the configuration of a SACM component or updating a target endpoint profile that resides on an evaluator. In essence, guidance is transported via the management plane.

Endpoint Hardware Inventory: The set of hardware components that compose a specific endpoint representing its hardware configuration.

Hardware Component: A distinguishable physical component used to compose an endpoint.

The composition of an endpoint can be changed over time by adding or removing hardware components. In essence, every physical endpoint is potentially a composite of multiple hardware components, typically resulting in a hierarchical composition of hardware components. The composition of hardware components is based on interconnects provided by specific hardware types (e.g. FRU in a chassis are connected via redundant busses). In general, a hardware component can be distinguished by its serial number. Occasionally, hardware components are referred to as power sucking aliens.

Information Element: A representation of information about physical and virtual "objects of interest".

Information elements are the building blocks that constitute the SACM information model. In the context of SACM, an information element that expresses a single value with a specific name is referred to as an Attribute (analogous to an attribute-value pair). A set of attributes that is bundled into a more complex composite information element is referred to as a Subject. Every
information element in the SACM information model has a unique name. Endpoint attributes or time stamps, for example, are represented as information elements in the SACM information model.

Information Model: An abstract representation of data, their properties, relationships between data and the operations that can be performed on the data.

While there is some overlap with a data model, [RFC3444] distinguishes an information model as being protocol and implementation neutral whereas a data model would provide such details. The purpose of the SACM information model is to ensure interoperability between SACM data models (that are used as transport encoding) and to provide a standardized set of information elements for communication between SACM components.

Interaction Model: The definition of specific sequences regarding the exchange of messages (data in motion), including, for example, conditional branching, thresholds and timers.

An interaction model, for example, can be used to define operations, such as registration or discovery, on the control plane. A composition of data models for data in motion and a corresponding interaction model is a protocol.

Internal Collector: A collector that runs on a target endpoint to acquire information from that target endpoint.

Management Plane: An architectural component providing common functions to steer the behavior of SACM components, e.g. their behavior on the control plane.

Typically, a SACM component can fulfill its purpose without continuous input from the management plane. In contrast, without continuous availability of control plane functions a typical SACM component could not function properly. In general, interaction on the management plane is less frequent and less regular than on the control plane. Input via the management plane can be manual (e.g. via a CLI), or can be automated via management plane functions that are part of other SACM components.

Network Address: A layer-specific address that follows a layer-specific address scheme.

The following characteristics are a summary derived from the Common Information Model and ITU-T X.213. Each Network Interface of a specific layer can be associated with one or more addresses appropriate for that layer. There is no guarantee that a network
address is globally unique. A dedicated authority entity can provide a level of assurance that a network address is unique in its given scope. In essence, there is always a scope to a network address, in which it is intended to be unique.

Examples include: physical Ethernet port with a MAC address, layer 2 VLAN interface with a MAC address, layer 3 interface with multiple IPv6 addresses, layer 3 tunnel ingress or egress with an IPv4 address.

Network Interface: An Endpoint is connected to a network via one or more Network Interfaces. Network Interfaces can be physical (Hardware Component) or logical (virtual Hardware component, i.e. a dedicated Software Component). Network Interfaces of an Endpoint can operate on different layers, most prominently what is now commonly called layer 2 and 3. Within a layer, interfaces can be nested.

In SACM, the association of Endpoints and Network Addresses via Network Interfaces is vital to maintain interdependent autonomous processes that can be targeted at Target Endpoints, unambiguously.

Examples include: physical Ethernet port, layer 2 VLAN interface, a MC-LAG setup, layer 3 Point-to-Point tunnel ingress or egress.

Metadata: Data about data.

In the SACM information model, data is referred to as Content. Metadata about the content is referred to as Content-Metadata, respectively. Content and Content-Metadata are combined into Subjects called Content-Elements in the SACM information model. Some information elements defined by the SACM information model can be part of the Content or the Content-Metadata. Therefore, if an information element is considered data or data about data depends on which kind of Subject it is associated with. The SACM information model also defines metadata about the data origin via the Subject Statement-Metadata. Typical examples of metadata are time stamps, data origin or data source.

Posture: Defined in [RFC5209] as "configuration and/or status of hardware or software on an endpoint as it pertains to an organization’s security policy."

This term is used within the scope of SACM to represent the configuration and state information that is collected from a target endpoint in the form of endpoint attributes (e.g. software/hardware inventory, configuration settings, dynamically assigned
addresses). This information may constitute one or more posture attributes.

Posture Attributes: Defined in [RFC5209] as "attributes describing the configuration or status (posture) of a feature of the endpoint. A Posture Attribute represents a single property of an observed state. For example, a Posture Attribute might describe the version of the operating system installed on the system."

Within this document this term represents a specific assertion about endpoint configuration or state (e.g. configuration setting, installed software, hardware) represented via endpoint attributes. The phrase "features of the endpoint" highlighted above refers to installed software or software components.

Provider: A provider is a SACM role assigned to a SACM component that provides role-specific functions to provide information to other SACM components.

Repository: A repository is a controller that contains functions to consume, store and provide information of a particular kind.

Such information is typically data transported on the data plane, but potentially also data and metadata from the control and management plane. A single repository may provide the functions of more than one specific repository type (i.e. configuration baseline repository, assessment results repository, etc.)

SACM Broker Controller: A SACM Broker Controller is a controller that contains control plane functions to provide and/or connect services on behalf of other SACM components via interfaces on the control plane.

A broker may provide, for example, authorization services and find, upon request, SACM components providing requested services.

SACM Component: Is a component, as defined in [I-D.ietf-i2nsf-terminology], that is composed of SACM capabilities.

In the context of SACM, a set of SACM functions composes a SACM component. A SACM component conducts SACM tasks, acting on control plane, data plane and/or management plane via corresponding SACM interfaces. SACM defines a set of standard components (e.g. a collector, a broker, or a data store). A SACM component contains at least a basic set of control plane functions and can contain data plane and management plane functions. A SACM component residing on an endpoint assigns one or more SACM roles
to the corresponding endpoint due to the SACM functions it is composed of. A SACM component "resides on" an endpoint and an endpoint "contains" a SACM component, correspondingly. For example, a SACM component that is composed solely of functions that provide information would only take on the role of a provider.

SACM Component Discovery: The task of discovering the capabilities provided by SACM components within a SACM domain.

This is likely to be performed via an appropriate set of control plane functions.

SACM Component Label: A specific endpoint label that is used to identify a SACM component.

In content-metadata, this label is called data origin.

SACM Content: The payload provided by SACM components to the SACM domain on the data plane.

SACM content includes the SACM data models.

SACM Domain: Endpoints that include a SACM component compose a SACM domain.

(To be revised, additional definition content TBD, possible dependencies to SACM architecture)

SACM Function: A behavioral aspect of a SACM component that provides external SACM Interfaces or internal interfaces to other SACM Functions.

For example, a SACM Function with SACM Interfaces on the Control Plane can provide a brokering function to other SACM Components. Via Data Plane interfaces, a SACM Function can act as a provider and/or as a consumer of information. SACM Functions can be propagated as the Capabilities of a SACM Component and can be discovered by or negotiated with other SACM Components.

SACM Interface: An interface, as defined in [I-D.ietf-i2nsf-terminology], that provides SACM-specific operations.

[I-D.ietf-i2nsf-terminology] defines interface as a "set of operations one object knows it can invoke on, and expose to, another object," and further defines interface by stating that an interface "decouples the implementation of the operation from its
specification. An interface is a subset of all operations that a
given object implements. The same object may have multiple types
of interfaces to serve different purposes."

In the context of SACM, SACM Functions provide SACM Interfaces on
the management, control, or data plane. Operations a SACM
Interface provides are based on corresponding data model defined
by SACM. SACM Interfaces are used for communication between SACM
components.

SACM Proxy Controller: A SACM Proxy Controller is a controller that
provides data plane and control plane functions, information, or
services on behalf of another component, which is not directly
participating in the SACM architecture.

SACM Role: Is a role, as defined in [I-D.ietf-i2nsf-terminology],
that requires the SACM Component assuming the role to bear a set
of SACM functions or interfaces.

SACM Roles provide three important benefits. First, it enables
different behavior to be supported by the same Component for
different contexts. Second, it enables the behavior of a
Component to be adjusted dynamically (i.e., at runtime, in
response) to changes in context, by using one or more Roles to
define the behavior desired for each context. Third, it decouples
the Roles of a Component from the Applications that use that
Component."

In the context of SACM, SACM roles are associated with SACM
components and are defined by the set of functions and interfaces
a SACM component includes. There are three SACM roles: provider,
consumer, and controller. The roles associated with a SACM
component are determined by the purpose of the SACM functions and
corresponding SACM interfaces the SACM component is composed of.

SACM Statement: Is an assertion that is made by a SACM Component.

Security Automation: The process of which security alerts can be
automated through the use of different components to monitor,
analyze and assess endpoints and network traffic for the purposes
of detecting misconfigurations, misbehaviors or threats.

Security Automation is intended to identify target endpoints that
cannot be trusted (see "trusted" in [RFC4949]). This goal is
achieved by creating and processing evidence (assessment
statements) that a target endpoint is not a trusted system
[RFC4949].
Software Package: A generic software package (e.g. a text editor).

Software Component: A software package installed on an endpoint.

The software component may include a unique serial number (e.g. a text editor associated with a unique license key).

Software Instance: A running instance of a software component.

For example, on a multi-user system, one logged-in user has one instance of a text editor running and another logged-in user has another instance of the same text editor running, or on a single-user system, a user could have multiple independent instances of the same text editor running.

State: A volatile set of endpoint attributes of a (target) endpoint that is affected by a reboot-cycle.

Local state is created by the interaction of components with other components via the control plane, via processing data plane payload, or via the functional properties of local hardware and software components. Dynamic configuration (e.g. IP address distributed dynamically via an address distribution and management services, such as DHCP) is considered state that is the result of the interaction with another component (e.g. provided by a DHCP server with a specific configuration).

Examples: The static association of an IP address and a MAC address in a DHCP server configuration, a directory-path that identifies a log-file directory, a registry entry.

Statement: A statement is the root/top-level subject defined in the SACM information model.

A statement is used to bundle Content Elements into one subject and includes metadata about the data origin.

Subject: A semantic composite information element pertaining to a system entity that is a target endpoint.

Like Attributes, subjects have a name and are composed of attributes and/or other subjects. Every IE that is part of a subject can have a quantity associated with it (e.g. zero-one, none-unbounded). The content IE of a subject can be an unordered or an ordered list.

In contrast to the definitions of subject provided by [RFC4949], a subject in the scope of SACM is neither "a system entity that
causes information to flow among objects or changes the system state" nor "a name of a system entity that is bound to the data items in a digital certificate".

In the context of SACM, a subject is a semantic composite of information elements about a system entity that is a target endpoint. Every acquirable subject—defined in the scope of SACM—about a target endpoint represents and therefore identifies every subject—defined by [RFC4949]—that is a component of that target endpoint. The semantic difference between both definitions can be subtle in practice and is in consequence important to highlight.

Supplicant: A component seeking to be authenticated via the control plane for the purpose of participating in a SACM domain.

System Resource: Defined in [RFC4949] as "data contained in an information system; or a service provided by a system; or a system capacity, such as processing power or communication bandwidth; or an item of system equipment (i.e., hardware, firmware, software, or documentation); or a facility that houses system operations and equipment."

Target Endpoint: Is an endpoint that is under assessment at some point in, or region of, time.

Every endpoint that is not specifically designated as an excluded endpoint is a target endpoint. A target endpoint is not part of a SACM domain unless it contains a SACM component (e.g. a SACM component that publishes collection results coming from an internal collector).

A target endpoint is similar to a device that is a Target of Evaluation (TOE) as defined in Common Criteria and as referenced by [RFC4949].

Target Endpoint Address: An address that is layer specific and which follows layer specific address schemes.

Each interface of a specific layer can be associated with one or more addresses appropriate for that layer. There is no guarantee that an address is globally unique. In general, there is a scope to an address in which it is intended to be unique.

Examples include: physical Ethernet port with a MAC address, layer 2 VLAN interface with a MAC address, layer 3 interface with multiple IPv6 addresses, layer 3 tunnel ingress or egress with an IPv4 address.
Target Endpoint Characterization: The description of the distinctive nature of a target endpoint, that is based on its characteristics.

Target Endpoint Characterization Record: A set of endpoint attributes about a target endpoint that was encountered in a SACM domain, which are associated with that target endpoint as a result of a Target Endpoint Characterization Task.

A characterization record is intended to be a representation of an endpoint. It cannot be assured that a record distinctly represents a single target endpoint unless a set of one or more endpoint attributes that compose a unique set of identifying endpoint attributes are included in the record. Otherwise, the set of identifying attributes included in a record can match more than one target endpoints, which are - in consequence - indistinguishable to a SACM domain until more qualifying endpoint attributes can be acquired and added to the record. A characterization record is maintained over time in order to assert that acquired endpoint attributes are either about an endpoint that was encountered before or an endpoint that has not been encountered before in a SACM domain. A characterization record can include, for example, acquired configuration, state or observed behavior of a specific target endpoint. Multiple and even conflicting instances of this information can be included in a characterization record by using timestamps and/or data origins to differentiate them. The endpoint attributes included in a characterization record can be used to re-identify a distinct target endpoint over time. Classes or profiles can be associated with a characterization record via the Classification Task in order to guide collection, evaluation or remediation tasks.

Target Endpoint Characterization Task: An ongoing task of continuously adding acquired endpoint attributes to a corresponding record. The TE characterization task manages the representation of encountered target endpoints in the SACM domain in the form of characterization records. For example, the output of a target endpoint discovery task or a collection task can be processed by the characterization task and added to the record. The TE characterization Task also manages these representations of target endpoints encountered in the SACM domain by splitting or merging the corresponding records as new or more refined endpoint attributes become available.

Target Endpoint Classification Task: The task of associating a class from an extensible list of classes with an endpoint characterization record. TE classes function as imperative and declarative guidance for collection, evaluation, remediation and security posture assessment in general.
Target Endpoint Discovery Task: The ongoing task of detecting previously unknown interaction of a potential target endpoint in the SACM domain. TE Discovery is not directly targeted at a specific target endpoint and therefore an un-targeted task. SACM Components conducting the discovery task as a part of their function are typically distributed and located, for example, on infrastructure components or collect from those remotely via appropriate interfaces. Examples of infrastructure components that are of interest to the discovery task include routers, switches, VM hosting or VM managing components, AAA servers, or servers handling dynamic address distribution.

Target Endpoint Identifier: The target endpoint discovery task and the collection tasks can result in a set of identifying endpoint attributes added to a corresponding Characterization Record. This subset of the endpoint attributes included in the record is used as a target endpoint identifier, by which a specific target endpoint can be referenced. Depending on the available identifying attributes, this reference can be ambiguous and is a "best-effort" mechanism. Every distinct set of identifying endpoint attributes can be associated with a target endpoint label that is unique in a SACM domain.

Target Endpoint Label: An endpoint label that identifies a specific target endpoint.

Target Endpoint Profile: A bundle of expected or desired component composition, configurations and states that is associated with a target endpoint.

The corresponding task by which the association with a target endpoint takes places is the endpoint classification task. The task by which an endpoint profile is created is the endpoint characterization task. A type or class of target endpoints can be defined via a target endpoint profile. Examples include: printers, smartphones, or an office PC.

In respect to [RFC4949], a target endpoint profile is a protection profile as defined by Common Criteria (analogous to the target endpoint being the target of evaluation).

SACM Task: Is a task conducted within the scope of a SACM domain by one or more SACM functions that achieves a SACM-defined outcome.

A SACM task can be triggered by other operations or functions (e.g. a query from another SACM component or an unsolicited push on the data plane due to an ongoing subscription). A task is part of a SACM process chain. A task starts at a given point in time.
and ends in a deterministic state. With the exception of a collection task, a SACM task consumes SACM statements provided by other SACM components. The output of a task is a result that can be provided (e.g. published) on the data plane.

The following tasks are defined by SACM:

Target Endpoint Discovery
Target Endpoint Characterization
Target Endpoint Classification
Collection
Evaluation [TBD]
Information Sharing [TBD]
SACM Component Discovery
SACM Component Authentication [TBD]
SACM Component Authorization [TBD]
SACM Component Registration [TBD]

Timestamps: Defined in [RFC4949] as "with respect to a data object, a label or marking in which is recorded the time (time of day or other instant of elapsed time) at which the label or marking was affixed to the data object".

A timestamp always requires context, i.e. additional information elements that are associated with it. Therefore, all timestamps wrt information elements are always metadata. Timestamps in SACM Content Elements may be generated outside a SACM Domain and may be encoded in an unknown representation. Inside a SACM domain the representation of timestamps is well-defined and unambiguous.

Virtual Endpoint: An endpoint composed entirely of logical system components (see [RFC4949]).

The most common example is a virtual machine/host running on a target endpoint. Effectively, target endpoints can be nested and at the time of this writing the most common example of target endpoint characteristics about virtual components is the EntLogicalEntry in [RFC6933].
Vulnerability Assessment: An assessment specifically tailored to determining whether a set of endpoints is vulnerable according to the information contained in the vulnerability description information.

Vulnerability Description Information: Information pertaining to the existence of a flaw or flaws in software, hardware, and/or firmware, which could potentially have an adverse impact on enterprise IT functionality and/or security.

Vulnerability detection information should contain enough information to support vulnerability detection.

Vulnerability Detection Data: A type of imperative guidance extracted or derived from vulnerability description information that describes the specific mechanisms of vulnerability detection that is used by an enterprise’s vulnerability management capabilities to determine if a vulnerability is present on an endpoint.

Vulnerability Management Capabilities: An IT management capability tailored toward managing endpoint vulnerabilities and associated metadata on an ongoing basis by ingesting vulnerability description information and vulnerability detection data, and performing vulnerability assessments.

Vulnerability assessment capabilities: An assessment capability that is tailored toward determining whether a set of endpoints is vulnerable according to vulnerability description information.

Workflow: A workflow is a modular composition of tasks that can contain loops, conditionals, multiple starting points and multiple endpoints.

The most prominent workflow in SACM is the assessment workflow.

3. IANA Considerations

This memo includes no request to IANA.

4. Security Considerations

This memo documents terminology for security automation. While it is about security, it does not affect security.
5. Acknowledgements

6. Change Log

Changes from version 00 to version 01:

- Added simple list of terms extracted from UC draft -05. It is expected that comments will be received on this list of terms as to whether they should be kept in this document. Those that are kept will be appropriately defined or cited.

Changes from version 01 to version 02:

- Added Vulnerability, Vulnerability Management, xposure, Misconfiguration, and Software flaw.

Changes from version 02 to version 03:

- Removed Section 2.1. Cleaned up some editing nits; broke terms into 2 sections (predefined and newly defined terms). Added some of the relevant terms per the proposed list discussed in the IETF 89 meeting.

Changes from version 03 to version 04:

- TODO

Changes from version 04 to version 05:

- TODO

Changes from version 05 to version 06:

- Updated author information.
- Combined "Pre-defined Terms" with "New Terms and Definitions".
- Removed "Requirements language".
- Removed unused reference to use case draft; resulted in removal of normative references.
- Removed introductory text from Section 1 indicating that this document is intended to be temporary.
- Added placeholders for missing change log entries.

Changes from version 06 to version 07:
o Added Contributors section.

o Updated author list.

o Changed title from "Terminology for Security Assessment" to "Secure Automation and Continuous Monitoring (SACM) Terminology".

o Changed abbrev from "SACM-Terms" to "SACM Terminology".

o Added appendix The Attic to stash terms for future updates.

o Added Authentication, Authorization, Data Confidentiality, Data Integrity, Data Origin, Data Provenance, SACM Component, SACM Component Discovery, Target Endpoint Discovery.

o Major updates to Building Block, Function, SACM Role, Target Endpoint.

o Minor updates to Broker, Capability, Collection Task, Evaluation Task, Posture.

o Relabeled Role to SACM Role, Endpoint Target to Target Endpoint, Endpoint Discovery to Endpoint Identification.

o Moved Asset Targeting, Client, Endpoint Identification to The Attic.

o Endpoint Attributes added as a TODO.

o Changed the structure of the Change Log.

Changes from version 07 to version 08:

o Added Assertion, Collection Result, Collector, Excluded Endpoint, Internal Collector, Network Address, Network Interface, SACM Domain, Statement, Target Endpoint Identifier, Target Endpoint Label, Timestamp.

o Major updates to Attributes, Broker, Collection Task, Consumer, Controller, Control Plane, Endpoint Attributes, Expected Endpoint State, SACM Function, Provider, Proxy, Repository, SACM Role, Target Endpoint.

o Minor updates to Asset, Building Block, Data Origin, Data Source, Data Provenance, Endpoint, Management Plane, Posture, Posture Attribute, SACM Component, SACM Component Discovery, Target Endpoint Discovery.
Changes from version 08 to version 09:

- Updated author list.
- Removed Building Block.
- Major updates to Control Plane, Endpoint Attribute, Expected Endpoint State, Information Model, Management Plane.
- Minor updates to Attribute, Capabilities, SACM Function, SACM Component, Collection Task.
- Moved Asset Characterization to The Attic.

Changes from version 09 to version 10:

- Added Configuration Drift, Data in Motion, Data at Rest, Endpoint Management Capability, Hardware Component, Hardware Inventory, Hardware Type, SACM Interface, Target Endpoint Characterization Record, Target Endpoint Characterization Task, Target Endpoint Classification Task, Target Endpoint Discovery Task, Vulnerability Description Information, Vulnerability Detection Data, Vulnerability Management Capability, Vulnerability Assessment
- Added references to i2nsf definitions in Capability, SACM Component, SACM Interface, SACM Role.
- Added i2nsf Terminology I-D Reference.
- Major Updates to Endpoint, SACM Task, Target Endpoint Identifier.
- Minor Updates to Guidance, SACM Component Discovery, Target Endpoint Label, Target Endpoint Profile.
- Relabeled SACM Task
- Removed Target Endpoint Discovery

Changes from version 10 to version 11:
Added Content Element, Content Metadata, Endpoint Label, Information Element, Metadata, SACM Component Label, Workflow.

Major Updates to Assessment, Capability, Collector, Endpoint Management Capabilities, Guidance, Vulnerability Assessment Capabilities, Vulnerability Detection Data, Vulnerability Assessment Capabilities.

Minor updates to Collection Result, Control Plane, Data in Motion, Data at Rest, Data Origin, Network Interface, Statement, Target Endpoint Label.

Relabeled Endpoint Management Capability, Vulnerability Management Capability, Vulnerability Assessment.

Changes from version 11 to version 12:

Added Configuration, Endpoint Characteristic, Event, SACM Content, State, Subject.

Major Updates to Assertion, Data in Motion, Data Provenance, Data Source, Interaction Model.

Minor Updates to Attribute, Control Plane, Data Origin, Data Provenance, Expected Endpoint State, Guidance, Target Endpoint Classification Task, Vulnerability Detection Data.

Changes from version 12 to version 13:

Added Virtual Component.

Major Updates to Capability, Collection Task, Hardware Component, Hardware Type, Security Automation, Subject, Target Endpoint, Target Endpoint Profile.

Minor Updates to Assertion, Data Plane, Endpoint Characteristics.

Changes from version 13 to version 14:

Handled a plethora of issues listed in GitHub.

Pruned some commonly understood terms.

Narrowing term labels per their definitions.

In some cases, excised expositional text.
Where expositional text was left intact, it has been separated from the actual definition of a term.

Changes from version 14 to version 16:
- moved obsolete definitions into the Appendix (attic).

7. Contributors
8.1. Normative References


8.2. Informative References


Appendix A. The Attic

The following terms are stashed for now and will be updated later:

Asset: Is a system resource, as defined in [RFC4949], that may be composed of other assets.

Examples of Assets include: Endpoints, Software, Guidance, or X.509 public key certificates. An asset is not necessarily owned by an organization.

Asset Management: The IT process by which assets are provisioned, updated, maintained and deprecated.

Asset Characterization: Asset characterization is the process of defining attributes that describe properties of an identified asset.

Asset Targeting: Asset targeting is the use of asset identification and categorization information to drive human-directed, automated decision making for data collection and analysis in support of endpoint posture assessment.

Client: An architectural component receiving services from another architectural component.

Endpoint Identification (TBD per list; was "Endpoint Discovery"): The process by which an endpoint can be identified.

Authors’ Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
Darmstadt 64295
Germany

Email: henk.birkholz@sit.fraunhofer.de