# Information Model Update

SACM WG Virtual Interim Meeting

06/15/2016

# Agenda

- Status
- Open issues
- Next steps

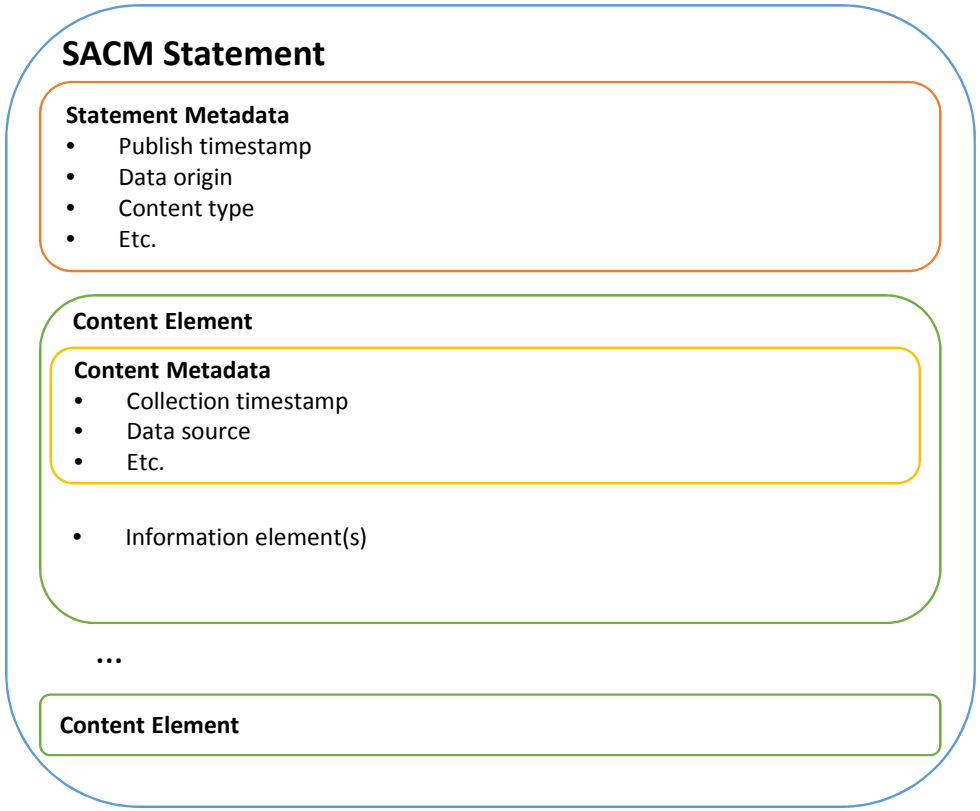
# Status

- Merged many of the changes from the I-D IM[1] into the WG IM[2]
- Posted a new draft on 6/8/16
- Still need to resolve the discussion around SACM statements and content elements[3]
- Still need to address IPFIX syntax concerns[4][5]

1. https://datatracker.ietf.org/doc/draft-camwinget-sacm-information-model/
2. https://datatracker.ietf.org/doc/draft-ietf-sacm-information-model/
3. https://www.ietf.org/mail-archive/web/sacm/current/msg04159.html
4. http://www.ietf.org/mail-archive/web/sacm/current/msg03906.html
5. http://www.ietf.org/mail-archive/web/sacm/current/msg03922.html

# Statement and content element

- Serves as an envelope to pass information between SACM components
- Contains metadata and one or more content elements
- Each content element contains one or more information elements
- Through nesting, they can track the progression of information between SACM components



# Mapping between SACM metadata and SWID M&A[1]

| SACM Metadata | SWID M&A |
|---|---|
| Globally unique identifier of statement | Not directly supported, but, a NEA Server could potentially generate and track this identifier upon the receipt of a message. |
| Data origin of statement | PB-PA header with PC and PV identifier. |
| Creation timestamp of statement | Two options here:<br>(1) Time the PC believes the change occurred. This can be obtained from the Event ID timestamp.<br>(2) Time when the message is published to the NEA Server. |
| Publication timestamp of statement | The time when the message is published to the NEA Server. |
| Type of content | PA subtype and tag version. |
| Creation timestamp of content | Four options:<br>(1) When the tag was created by the vendor?<br>(2) When the tag was dropped on the endpoint?<br>(3) When the tag was generated by a package database?<br>(4) Last recorded event on a tag? |
| Data source of content | Machine certificate via TLS and SWID 2015 device identifier. |

1. https://datatracker.ietf.org/doc/draft-coffin-sacm-nea-swid-patnc/

# Mapping between SACM metadata and OVAL[1]*

| SACM Metadata | OVAL |
|---|---|
| Globally unique identifier of statement | None. |
| Data origin of statement | Generator element contains information about the product that produced the OVAL document, but, it would likely be too generic. |
| Creation timestamp of statement | Timestamp in the Generator element states when the OVAL document was created. It is not necessarily when the information in the document was collected or evaluated (although it could be). |
| Publication timestamp of statement | Timestamp in the Generator element states when the OVAL document was created. Again, it is not necessarily aligned with when it was published (although it could be). |
| Type of content | Generator element contains the version of OVAL that the document is expressed in. |
| Creation timestamp of content | OVAL does not track when individual pieces of information were collected from the endpoint and represented as OVAL although the timestamp in the Generator element could potentially be used in this manner. Again, it may or may not be very accurate. |
| Data source of content | There is a System Information element that contains various identifying attributes about the endpoint from which the information was collected. However, there is not a unique identifier to represent the endpoint. As a result, a matching algorithm would likely need to be employed. |

1. https://datatracker.ietf.org/doc/draft-hansbury-sacm-oval-info-model-mapping/

* If PA-TNC was extended to support an OVAL-based data model, this mapping would be more aligned with SWID M&A

# Decisions to be made

- Let's try to solve this in the context of SWID M&A since it was recently adopted :)

- Do we want to require solutions to capture SACM metadata in explicit statement and content element structures in the payload? Or, do we want to leave it as a decision for the solution implementers to make?

- Creation timestamp of statement
  (1) Time the PC believes the change occurred. This can be obtained from the Event ID timestamp.
  (2) Time when the message is published to the NEA Server.

- Creation timestamp of content
  (1) Time when the tag was originally created by the vendor.
  (2) Time when the tag was dropped on the endpoint.
  (3) Time when the message was published to the NEA Server.
  (4) Time of the last recorded event on a tag (e.g. when a tag was updated).

# Next steps

- Reach consensus on whether or not we need explicit SACM statements and content elements
- Finish addressing the IPFIX syntax concerns
- Clean up Sections 5 through 7 and the appendices
- Send out an updated version of the WG IM in advance of IETF 96