SWID Message and Attributes for PA-TNC

draft-coffin-sacm-nea-swid-patnc-02

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

SACM Virtual Interim Meeting

September 13, 2016

Agenda

- Latest Revision
  - Flexible data model
  - Software Identifiers
  - Record Identifiers
  - Examples
  - Nominal Data Flow
  - Discussion Topics
- Next Steps

Latest Revision

- Released version -02 on Monday, September 12
- Generalizes the prior specification's assumption that data is normalized to use SWID tags
  - Requested at IETF 96
  - New title of document is Software Message and Attributes for PA-TNC
- Data model of information in messages is now flexible
  - Defines a new IANA table of supported data model types
  - Response attributes include a new field to report the data model used to express contained content

Software Data Model IANA Registry

- Each type of data model is assigned a 1-byte integer
  - This is used in messages to identify the data model used
- Reported data must be converted to a supported data model for delivery
  - Document still assumes there can be multiple data sources
- Specification currently defines 2 supported data models
  - ISO 2015 SWID Tags using XML
  - ISO 2009 SWID Tags using XML
  - More can be added

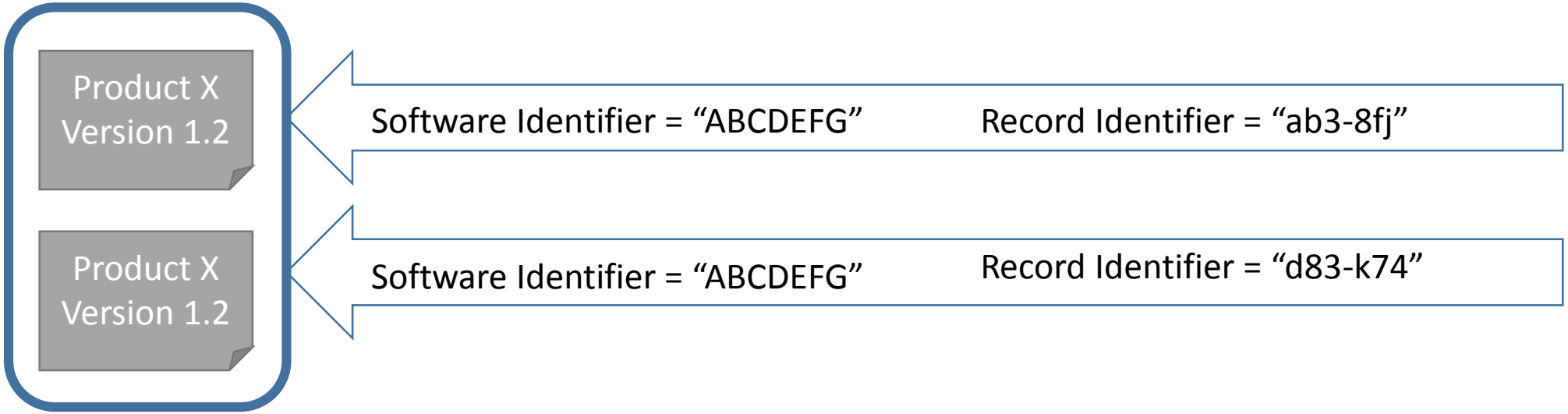
Software Identifiers

- “Software Identifiers” replace “SWID Tag Identifiers”
  - Still uniquely identifies a Software Product and Version
- Each software record (software data collected by the endpoint) has an associated Software Identifier
  - But the same Software Identifier can be associated with multiple software records
- Each data model defines a procedure for deriving a Software Identifier
  - Means that the same software product will have a different Software Identifiers under different data model

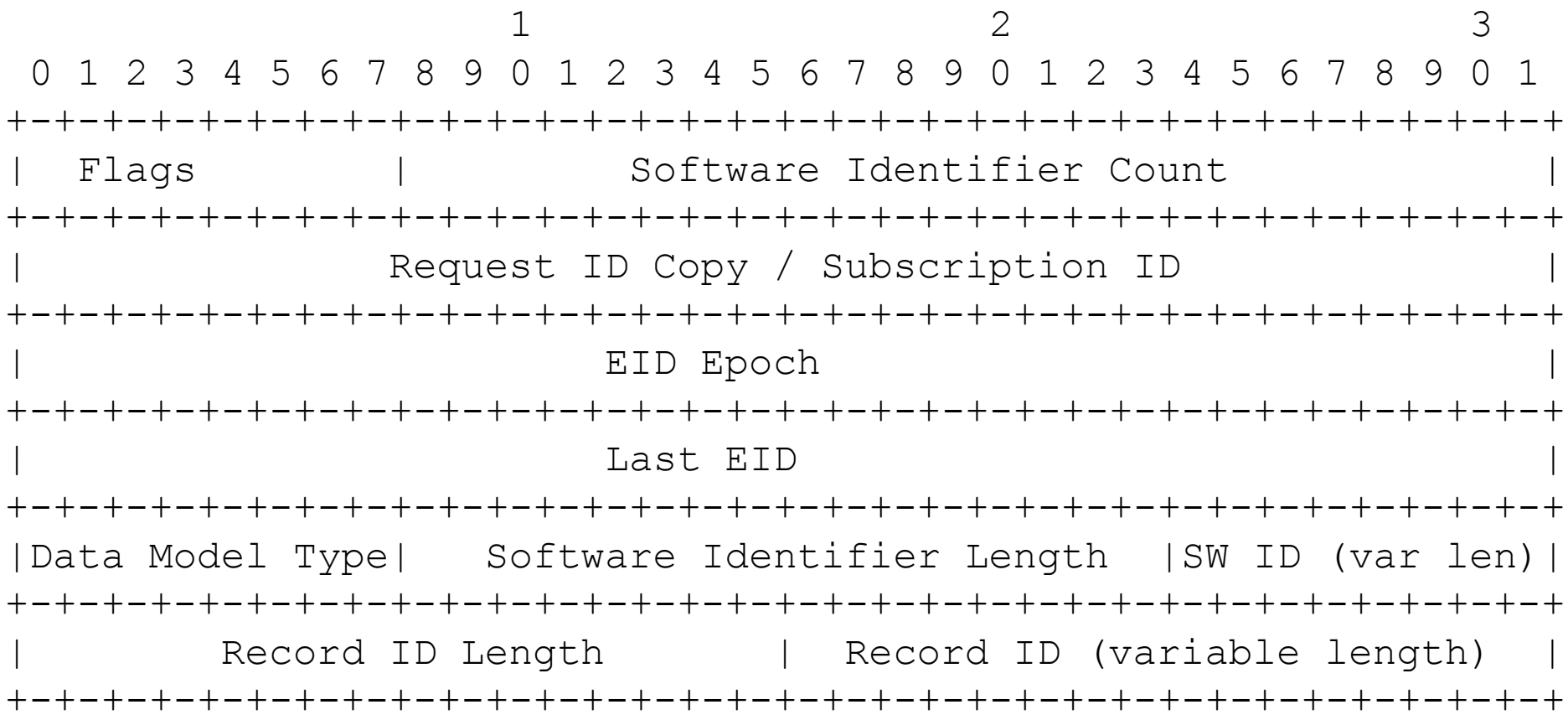
Record Identifiers

- Each software record collected by an endpoint is given a unique Record Identifier
  - Serves the same purpose as the old Instance Identifier

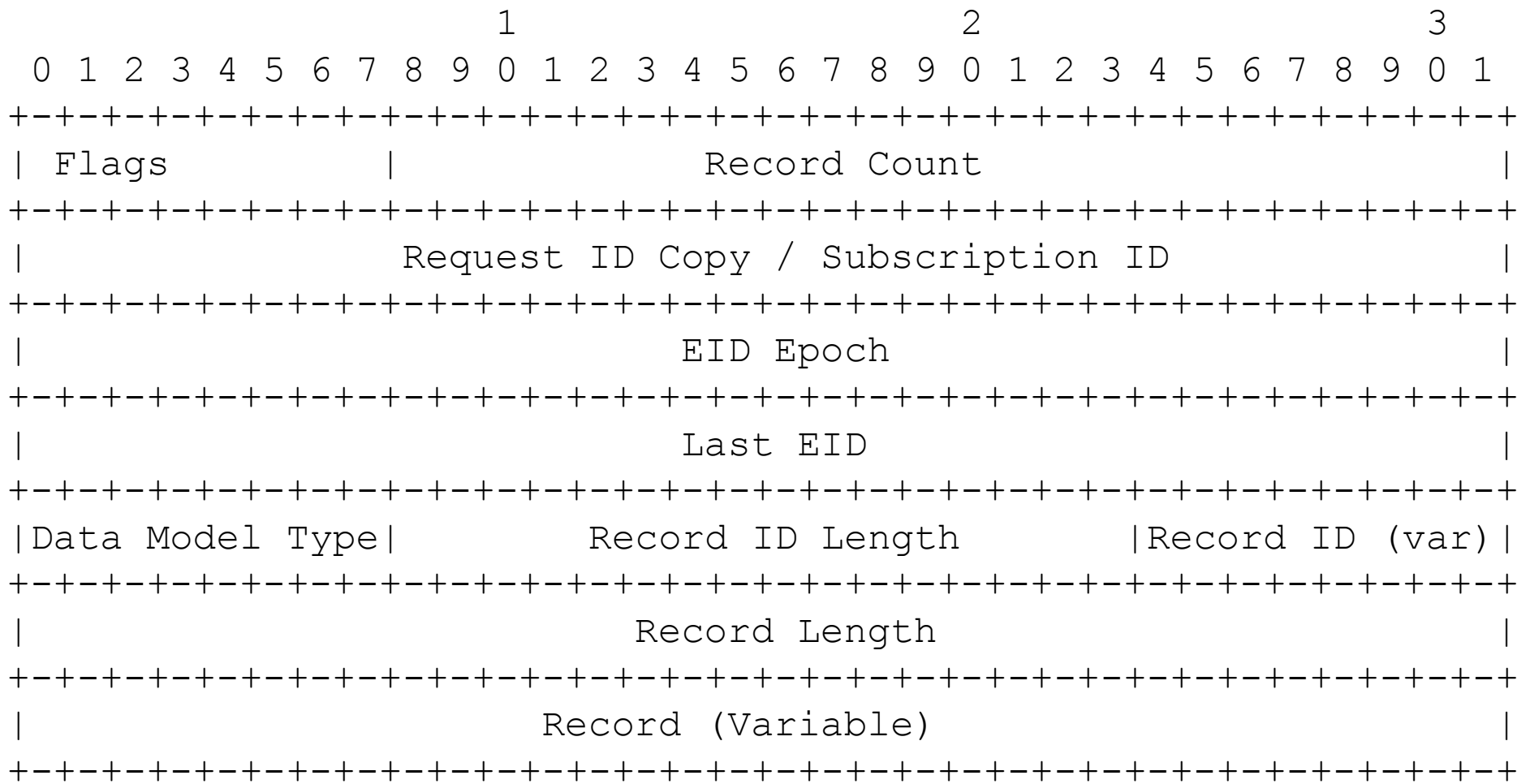
- Can be used to distinguish between multiple installation instances of a single software product



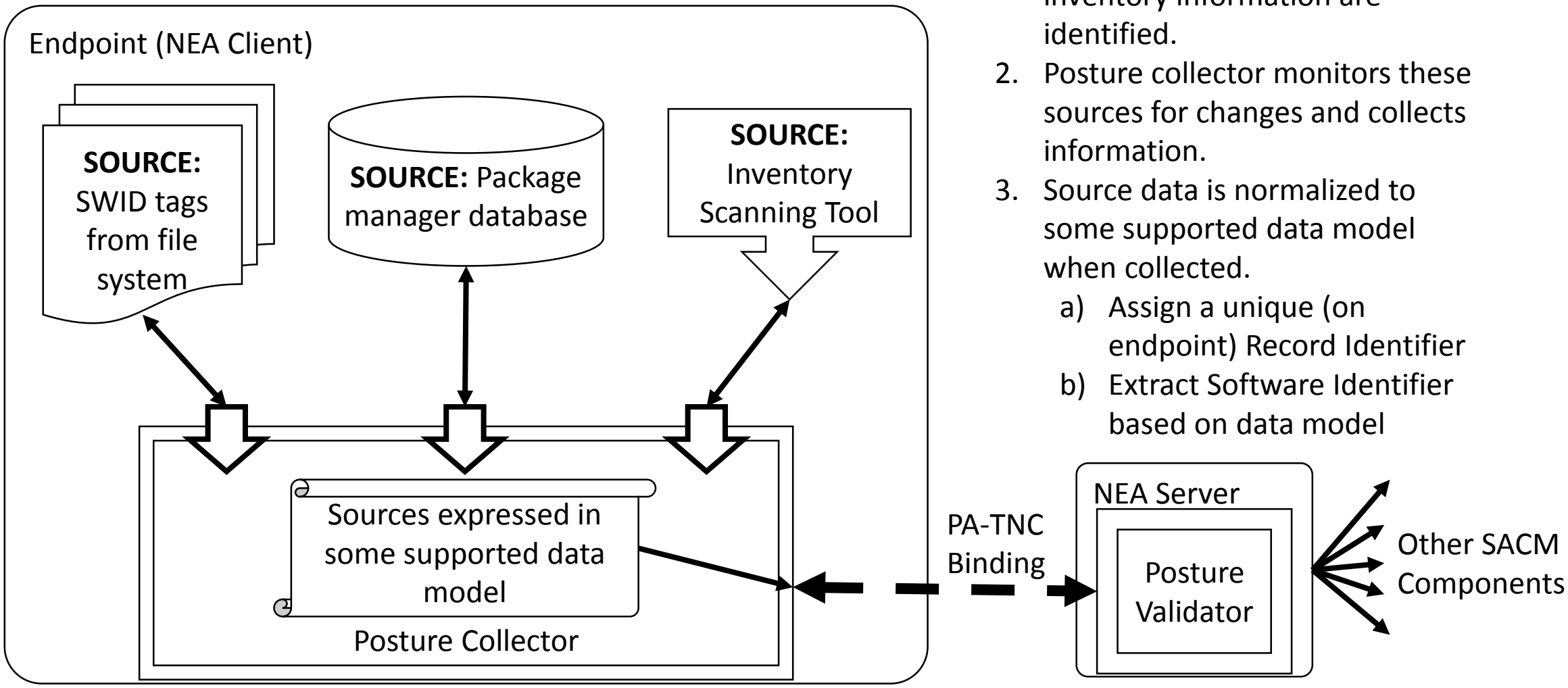
Software Identifier Inventory



Software Inventory



Nominal data flow



1. One or more sources of inventory information are identified.
2. Posture collector monitors these sources for changes and collects information.
3. Source data is normalized to some supported data model when collected.
   a) Assign a unique (on endpoint) Record Identifier
   b) Extract Software Identifier based on data model

* Sources are provided as examples. This slide makes no assertions as to any source being required.

Net result of changes

- Only real change is the ability to send software information using one of multiple data models
  - Data Model Type field allows up to 256 software data models to be identified, which hopefully is overkill

- All other functionality remains the same
  - Deliver event list or inventory
  - Deliver full records (ne tags) or identifiers
  - Targeted requests (targeted by Software Identifiers)
  - Support for subscriptions
  - Distinguish between multiple instances of a single software product

Possible topics for discussion

- Current assumption is that we are reporting installed software
  - On list there was discussion of reporting software packages (regardless of installation status) and/or running software

- There was a proposal to track data sources (prior to data normalization)
  - Software Identifiers are derived from software records
  - Two sources might populate software records for the same software product differently
  - Therefore, even if using the same data model, the software product might have different Software Identifiers from different sources

Next steps

- Continue discussions on-list