IETF 93 SACM Notes

Full minutes exist below, and these first two pages provide an overview. Thank you to Chris Inacio and Danny Haynes for taking notes, and to Jim Schaad for being our Jabber scribe.

Session I - Monday, July 20

We started the meeting with the traditional Note Well viewing and agenda bashing. During the agenda bashing our AD, Kathleen Moriarty, asked why we didn't have any protocols - specifically XMPP Grid[1] - to be discussed on the agenda, as we have a November 2015 milestone to adopt as a WG document at least one Protocol/Interface submission instantiating the SACM Architecture.

During the discussion that followed, Kathleen suggested that the XMPP-Grid submission could go into another working group to accommodate a wider set of use cases in the security automation space - not just for endpoint compliance but for information sharing as well.

The way that settled is somewhat ambiguous. But, what was clear is that, as a WG, SACM needs to make better progress on its drafts.

Then, we carried on with the agenda with one minor change, which placed Linda Dunbar's presentation ahead of others for logistical reasons.

- **NEA Assessment (Linda Dunbar):** NEA is narrower in scope than SACM but could be applied to a subset of what SACM would like to cover.
- **SACM Requirements (Lisa Lorenzin):** Brief review of where we are followed by a call for participation in knocking out most of the open issues during the week - several did.
- **SACM Terminology (Henk Birkholz):** Draft is far from complete and needs attention on some critical terms, such as posture, capability vs. function, and so on. We need draft-level coordination as well, as this draft supports the others.
- **SACM Architecture (Nancy Cam-Winget):** Recognition of work needing to be done, specifically that we need at least one methodology to implement for the sake of interoperability.
- **SACM Information Model (Lisa Lorenzin):** This is a work in progress, and we should consider better tracking of the topics that need covering - it's a large space.
- **OVAL Assessment (Danny Haynes):** OVAL is something usable as a starting point - something to examine, learn from, and apply in pieces. IPR issues are being worked, but IPR rights have not yet transferred.
- **ECP Mapping (Danny Haynes):** ECP has mapped to several SACM use cases, but needs to be extended to be complete; needs reviewers; has IPR considerations.

We then considered the working plan for the week which was to make as much progress as possible on the Requirements, Architecture, and Terminology drafts as a priority, but also to come up with an actionable set of topics requiring discussion within the Information Model at least via the mailing list.

---

[1] http://datatracker.ietf.org/doc/draft-salowey-sacm-xmpp-grid/

Session II - Friday, July 24

By this time we had worked to close all the issues against the Requirements draft, worked to further our shared understanding of the Architecture draft, and the Terminology draft. We also saw a presentation on plasma from Jim Schaad. Throughout there were specific calls to action for the WG to review documents - in particular the Architecture.

The Way Forward was discussed, and we decided that we would have time for only one virtual interim between IETF 93 and 94. Then, we ran through some proposals for another set of milestone updates, which follow:

> May 2015 Complete WGLC for Requirements
> Jul 2015 Complete WGLC for Architecture
> Sep 2015 Submit Requirements to IESG (if decided by WG)
> Nov 2015 WGLC Architecture
> Jan 2016 Submit Architecture to IESG
> Jan 2016 WGLC Information Model
> Mar 2016 Complete WGLC for Information Model
> Mar 2016 Adopt at least one Protocol/Interface submission
> May 2016 Adopt at least one Data Model submission
> Aug 2016 Submit Information Model to IESG
> Aug 2016 Update WG Milestones based on progress

These milestones need to be discussed on the mailing list before they are put into effect.

Notes from Chris Inacio
20-July-2015 (Session I)
- protocol work / november target
  - AD would like a discussion on XMPP protocol draft
    - checking for available people to present / review draft
    - Danny Hayes - ECP Mapping, not quite a protocol, but talks about TNC mapping
    - AD - does group need help for protocol review?
      - Adam M. (WGC) - problem has been more about parallelizing work in the group, not a lack of expertise
    - Jim Schaadt - Requirements & Architecture still too fluid to review a protocol
    - Dan R - agree, requirements getting pretty firm, architecture still in flux
  - AD Industry has a problem (CARIS meeting)
    - 3 protocol possibilities
      - RID
        - doesn't scale
      - TAXII
        - interoperability hard
        - hard to scale
      - XMPP Grid
        - does scale
        - at least 10 vendors using it
        - has federation, scales well, pub/sub native
        - needs to finish implementation
  - AD might be good to publish XMPP/Grid with multiple applicability to WG's (MILE, SACM, etc.)
    - Nancy CW - will work update with more applicability, different data models
  - Lisa L - should XMPP/Grid be done in XMPP WG?
    - AD - fine to do work here, or MILE

SACM / NEA comparison
- Linda D - presenter
- novice review across all the NEA / SACM drafts
  - Nancy CW - feedback

- NEA -> enterprise focus on endpoint performing an assessment for access control
- SACM -> more broad, want to share assessment & information for generating an assessment
- novice review of TNC / SACM
  - TNC is much larger framework
  - Lisa L - TNC for SACM draft author, provided draft as background from TNC work to SACM
  - quite different, but SACM is more focused, data point & protocols
  - Lisa L - can map various TNC elements to SACM implements
  - Linda D - is complete TNC widely deployed?
    - Lisa L - very few vendors have complete TNC implementation, but that's like asking if any vendors implemented 100% of the RFC's
      - meant to generate an interoperable set of standards

Requirements Draft
- Lisa L - presenter
- Still 9-12 open issues
- Interested in a working issue on the remaining open issues
  - at least 3 people
  - Nancy CW - Jim should be in the session
- Would like to present them to the list & WG on Friday to close out issues

Terminology
- Henk B - presenter
- Far from complete currently
- A few issues listed on GitHub still left
  - some small
  - some are very significant
- definition of posture
  - complex set of definitions to create posture definition
  - Lucy Linch - word constellations is used a number of times and not defined anywhere
- pub/sub not introduced in either Arch draft or Terminology draft
  - captured in GitHub on Arch draft
- capability vs. functions

- - not used intuitively in the Arch draft

Architecture

- Nancy CW - presenting
- Send email to Nancy to get on webex after this week to resolve arch issues
  - Dan (WGC) - we're in the same city, can we get together
  - Nancy - should focus on requirements
  - Lisa L - will build doodle pole to try to get time for everyone
- largest substantial GitHub issue
  - interoperability between providers/consumers not supporting same data model
  - Nancy CW - we should be defining a single mandatory to implement DM
- Henk B - presenting (where is the repository, nowhere? everywhere?)
  - repository is everywhere
  - Lisa L - would really like to see an outline of this seciton
    - thinks this would be really helpful
  - Nancy CW - thinks you are likely making an example of the arch, not changing it
  - will try to put something together by Friday

Information Model

- Lisa L - presenting
- most work on IM done via endpoint ID design team
- what does it mean to construct an identity
- two large areas still missing in endpoint ID design
  - relationships between attributes
  - metadata about those attributes observed to indentify an endpoint
- Lucy Linch -
  - privacy / confidentiallity is not covered in the IM, needs to get covered
  - AD - has to get covered, will get held up at IESG until resolved
  - Henk B - do not try to identify an endpoint here, but something that can be used to associate with other data
    - hash for example, which can be used

- Lisa L - agrees, maybe not calling it an "endpoint identity" but a rendezous point, to coordinate information collection processing
- Dan (WGC) - doesn't matter what you call it, just change it in the IM document
- Dan (WGC) - need to get IM model document sooner rather than later in order to meet November deadlines
- Launch mailing list discussion on IM draft to progress

SACM IM / OVAL Mapping

- Danny H - presenting
- OVAL
  - expected state
    -
  - actual state
    - OVAL term: results model
  - evaluation of comparison
- CyBOX
  - have we considered other data models
  - yes, might want to consider more data models
    - DMTF CIM, YANG,
- Scaling
  - language scaling
    - have to modify the language everytime you need to expand sources of data (registry keys, etc.)
  - XML document based
    - documents get VERY complex
    - hard to handle from humans
    - lots of ambiguities in the langage
      - makes scaling deployment challenging
- Level of abstraction
  - describes what to collect and how to collect it
    - separation of evaluation from collection is a good plan
  - important to keep abstraction in order for easy expansion of new platforms
- OVAL value adds:
  - OVAL System Characteristics
  - OVAL Definitions models

- both will need modification to effectively fulfill SACM
        - MITRE interested if its wanted would like to work on a plan
- AD - would like to see it move forward, poll on if its needed
    - Juan G - DHS owns IPR, working on getting that transferred
    - Lisa L - what is the end goal?
        - Danny H - OVAL might be a good place to START for SACM data models
            - would like to resolve lessons learned
        - two different pieces 1 including lessons learned into IM 2 creating a data model based on OVAL as a data model
    - Nancy CW - logistics
        - we're working on the requirements, XMPP/Grid, etc.
            - should we have some process for matching proposals against requirements?

- Mapping ECP to SACM
    - End Point Compliance Protocol
        - does have IPR
        - TCG is willing to contribute
- version of ECP currently published
    - primarily focused on "compliance to connect"
    - but EXTENSIBLE can be used for other use cases

IMC: integrity measurement collector IMV: integrity measurement validator Server Discovery and Validation: TCG (not IETF) protocol to find and validate a sever
- mapped ECP to 4 SACM use cases
- why use ECP and NEA/TNC in SACM
- way ahead
    - Dan (WGC)
        - how do we determine if this fits with SACM?
    - Danny H
        - more people to read the specs
        - should they attempt a mapping to the architecture?

Plan for the week
- requirements discussion / draft resolution
    - Lisa L - leading that effort
    - Lisa L - sending out doodle pole for times

- requirements time
- arch time
- terminology time
- might change Friday agenda

Notes From Danny Haynes

```
==================================================
==================================================
IETF 93
SACM Session I (1:00 PM CEST - 3:00 PM CEST)
July 20, 2015
Prague, Czech Republic
Minute taker #1: Chris Inacio
Minute taker #2: Danny Haynes
Jabber scribe: Jim Schaad

==================================================
Agenda Bashing (Dan Romascanu / Adam Montville)
==================================================
```

[Dan Romascanu]: Linda Dunbar made a request that she go first for her
NEA Assessment session. There were no objections so the original
agenda was modified to accommodate this request.

```
==================================================
Working Group Status (Dan Romascanu / Adam Montville)
==================================================
```

[Dan Romascanu]: The Use Cases draft is in the RFC Editor queue.
Thanks to David Waltermire and others for getting the last two issues
resolved. We are not doing that good on milestones. We have missed
the first three (Requirements WGLC, Architecture WGCL, and submit the
Requirements to the IESG).

[Kathleen Moriarty]: Will we be discussing any protocol submissions
such as XMPP-Grid since I will be bringing it up at the plenary?

[Chris Inacio]: Nancy is not here.

[Lisa Lorenzin]: She left early.

[Danny Haynes]: While not a protocol submission, in the ECP Mapping
session, we will be discussing the NEA/TNC specifications which could
eventually lead to a protocol submission.

[Dan Romascanu]: We are close to closure on the Terminology draft.

[Kathleen Moriarty]: Do we need more people involved with protocols
since most people here are familiar with data models?

[Adam Montville]: I wouldn't assume that. We have trouble working on more than one thing at a time. I think it is more of a time constraint issue than a capability gap.

[Jim Schaad]: The Requirements and Architecture drafts are too fluid to make this determination.

[Dan Romascanu]: Same situation. The Requirements draft is near being closed. The Architecture draft is not really near being closed. It is definitely a matter of bandwidth and protocol people with SACM context.

[Kathleen]: I think there is some crossover between incident response and information security.

[Lisa Lorenzin]: I think it would be good to be accepting a protocol, but, we need to have the Requirements and Architecture drafts ready first.

[Kathleen Moriarty]: Industry has a problem with information sharing. I made SOFIE**** and then RID. Then, MITRE created TAXII which looks a lot like RID. TAXII doesn't scale. RID has people using it and XMPP-Grid is an opportunity for us by building a mesh network.

[Lisa Lorenzin]: I wanted to make sure that that we understand the problem. We need to have vendors in the room to tell us what they need.

[Kathleen Moriarty]: SACM may be the place to do this work.

[Nancy Cam-Winget]: We may be able to submit it to show applicability in other working groups (MILE, etc.).

[Kathleen Moriarty]: Yes, keep it generic, but, show applicability to multiple areas. I am going to raise this at the plenary and you have your November timeline.

[Juan Gonzalez]: SACM is a place for work. There is an implementation report and it would be good to hear from vendors to better understand the needs of industry.

[Lisa Lorenzin]: SACM is endpoint compliance, but, would we better off to do XMPP-Grid in an XMPP-related WG?

[Kathleen Moriarty]: No, you can do work in other WGs.

[Lisa Lorenzin]: I feel like this is pushing XMPP-Grid on the WG
before we are ready.

[Kathleen Moriarty]: We should just see it and work through it to see
if we can use it. This is more of a heads up before going into the
plenary.

[Lisa Lorenzin]: Understood and it's not that I don't want to do the
work, but, we have a serialization problem.

[Dan Romascanu]: We need to see XMPP-Grid maps to the Requirements
draft and if it fits in here. Linda Dunbar will go now.

==
NEA Assessment (Linda Dunbar)
==
[Linda Dunbar]: In this session, I will be comparing SACM with NEA/
TNC. Please note that I am not an expert on these specifications so
this review is from a novice perspective. NEA is needed for
enterprise networks and SACM is more than that.

[Nancy Cam-Winget]: I spoke a lot about enterprises and initiating an
assessment and authorizing an endpoint to access a network. The
biggest difference is NEA performs and assessment. SACM is broader
than that. NEA is focused on network access where SACM is broader and
wants to be able to share that information and data. NEA is not
restricted to posture information.

[Linda Dunbar]: Can NEA be used in SACM?

[Nancy Cam-Winget]: Yes, a subset of it. NEA could be used for part
of it.

[Linda Dunbar]: TNC is a superset of NEA and we hope we don't use it
all.

[Lisa Lorenzin]: On the topic of TNC and SACM, the Policy Decision
Point (PDP) would be a SACM component and a client would be an access
requestor.

[Linda Dunbar]: Is TNC widely adopted?

[Lisa Lorenzin]: You could use TNC to implement SACM. There are
adopters, but, asking if they support all of TNC is like saying do you
support all RFCs in the IETF. Vendors support the specifications that
they need.

```
==================================================
Requirements (Lisa Lorenzin)
==================================================
```

[Lisa Lorenzin]: We had 20 open issues. The latest revision of the draft closes 11 of them. We are not going to work through the issues here in detail, but, instead are going to have a working meeting this week.

[Dan Romascanu]: Is this draft ready for WGLC?

[Lisa Lorenzin]: Yes. So, who is interested in having a working meeting this week? We will get together to figure out a schedule.

[Nancy Cam-Winget]: Make sure that Jim Schaad is included.

[Lisa Lorenzin]: Yes, he raised his hand.

```
==================================================
Terminology (Henk Birkholz)
==================================================
```

[Henk Birkholz]: There is still a lot of work to do on the Terminology draft and some of the issues transcend the draft. I am now going to go through some of the major issues. Posture is not defined although we have been talking about it for a while now. No relationships are defined. Attributes do not exist alone. We could go with a triple: subject, predicate, object.

[Lucy Lynch]: The term "constellations" is used in several places, but, not defined anywhere.

[Henk Birkholz]: Yes. We may have incompatible drafts.

[Dan Romascanu]: We may need draft-level coordination among editors.

[Henk Birkholz]: We tried to get the low-hanging fruit first. We also need to figure endpoint assertions, etc. I made a controversial proposal with representing it in Section 3 of the Architecture draft. I found an issue with the architecture which shows how the Terminology draft spans other drafts. One area I want to highlight is "capability" versus "function". Capabilities use models in the architecture whereas functions are software modules that accomplish something. Capabilities are active functions. Functions are also control plane specific. If you read the drafts and don't understand, please add a tracker.

[Dan Romascanu]: You said we are not done. I just wanted to remind everyone that we are not expecting this to be done quickly because it supports other documents. We don't have to finish this draft immediately.

[Henk Birkholz]: This definitely has a larger scope.

```
==================================================
Architecture (Nancy Cam-Winget)
==================================================
```

[Nancy Cam-Winget]: We are trying to focus on availability and consumption. We need a management control plane for who can be a provider, consumer or both. When we talk about different attributes there may be filters to limit the type of information that is exposed to the consumer. The notion of having the controller allow for management functions. This gets into deployment considerations and you may have a proxy. Functions can be broker, proxy, or repository. I think Jim Schaad responded to this which is different than what Henk said. We still need to clarify roles and interfaces and the Terminology draft still needs more work. The status of the architecture draft is that we missed a few issues from Henk Birkholz and Jim Schaad. Henk Birkholz will go over them. We don't have time for a line-by-line discussion this week, but, we can have a WebEx so that we can close them out.

[Dan Romascanu]: For clarification, can we not meet because of everyone's schedules? We might be able to have a session Friday morning.

[Lisa Lorenzin]: I will make a Doodle poll for the rest of the week. Just mention if you are focused on the Requirements or Architecture drafts.

[Nancy Cam-Winget]: The biggest one that we need to solve is with respect to interoperability. We need to define at least one methodology to implement for interoperability. It is in our charter to define one methodology to implement. Henk had some thoughts.

[Henk Birkholz]: Interfaces of SACM components aggregating multiple assessments to do a single assessment. Why can we define a repository as an entity because they can be in all SACM components? Most are actually building blocks about what makes a SACM component. At least, there are opportunities in the data plane and control plane. There are more general functions like evaluation, collection, etc. Having this component aspect and modularity about how components interact can be elaborated in how they are row could be beneficial for SIEM or IDS systems. I came to that conclusion.

[Lisa Lorenzin]: I would really like to see an outline of this proposal you described.

[Nancy Cam-Winget]: I am not sure you are changing the section rather than showing an example.

[Henk Birkholz]: Maybe before this.

[Lisa Lorenzin]: I think it would be best to show the outline to the group.

[Dan Romascanu]: Can you have it ready for Friday?

[Henk Birkholz]: I will try.

```
================================================
Information Model (Lisa Lorenzin)
================================================
```

[Lisa Lorenzin]: The primary progress is in the Endpoint ID Design Team and what it means to construct an identity. Cliff Kahn made an outline and we are now working to put issues from the design team in GitHub. We are close to figuring out identifying attributes. Then, we need to figure out relationships and metadata about these attributes (e.g. it would be good to know the MAC address is linked to the local interface). We are planning to determine if we should continue work in the Endpoint ID Design Team or if we should create a new design team.

[Henk Birkholz]: We would like to encourage people to join and participate in the Endpoint ID Design Team.

[Lisa Lorenzin]: Yes, this would be valuable.

[Lucy Lynch]: Privacy considerations should be included as well as confidentiality. It is mentioned, but, it is not described anywhere.

[Kathleen Moriarty]: Yes, we need to cover it.

[Henk Birkholz]: We don't compose an identity rather associate an endpoint with other events. You could also hash the values and not ever go back. Need to re-identify and may not be necessary.

[Lisa Lorenzin]: We want a rendezvous for identifying attributes or events about endpoint rather than identifying an actual endpoint.

[Dan Romascanu]: Make sure the problem is written down. What are the remaining issues and principle issues that need to be dealt with? This may be draft before it goes to WGLC.

[Lisa Lorenzin]: The work in the Endpoint ID Design Team focused on the Information Model, but, now the work is much broader.

[Dan Romascanu]: We need a plan. Can we have one for the end of the week?

[Lisa Lorenzin]: I am working on it.

[Dan Romascanu]: Can we count on this for Friday?

[Lisa Lorenzin]: No.

Notes from Chris Inacio
24-July-2015 (Session II)

Requirements Doc

Lisa presenting
- no more open issues in the requirements doc
- *walked through the various issues closed during the week - see GitHub*
- (WGC) are we using correct data modeling terms?
  - not synchronized across areas / WG
  - file a GitHub bug against req documnets for standardizing those terms
  - (AD) came up in SAG, no solution yet
  - (AD/WGC) have to work in coordination with ART area
- no questions/problems with closed issues
- would like to go to WGLC on document, but not submit too quickly
  - allow flexibility to update the document while evolving other documents
  - (AD) whatever the working group decides in this regard is fine
    - working group can discuss pros/cons on these documents
  - Jim S
    - doesn't matter too much which way we go
    - 1 detriment - would like to get wider view beyond SACM
      - (WGC) there is a way to ask for early review, so you get external review
      - (WGC) can do request for early review, and manage process

Architectural doc
24-July-2015
- still 14 open issues in GitHub
- need to make some decisions on moving forward
  - term capabilities vs. functions vs. role
    - role is composed of functions
      - what role you play is determined by the set of functions you implement

- - restructured document to reflect this change in terminology of functions & roles
  - (WGC) have created inconsistencies between I2NSF terminology
  - (WGC) why did you change the title "reference architecture" to "architecture"
    - a reference architecture is an implementation of the defined abstract architecture
- changed the names "posture consumer" and "posture provider" to "consumer"/"provider"
  - because posture information is just a specialized data type, could be used to carry other information
  - (AD) not necessary to make the change from comments
  - the AD comments changed point of view of how to build/define the system
- Added a lot of text to the introduction overview
  - looking for feedback
- simplified the labels in the diagram
- added new section 6 ("Component Capabilities")
  - please review
- polling room on concerns about the restructering the document
  - none given in the room
  - [ed] take to the list?
  - would like to schedule phone calls / follow up meetings to move arch forward
    - (WGC) which format virtual interim or design team format
      - lisa - likes the way the design team has worked
      - (WGC) - difference is that virtual interim lead by WGC, design team lead by limited power other person
    - henk - logisitics of weekly meeting of 2 hours for design team meetings is too much time
      - (WGC) design teams get to decide independently what they want to do
    - lisa - can't support weekly 2 hour call any longer either
    - lisa - virtual interm required to take and publish notes / design team is not

- adam - would like more aschronously, which means less / no phone calls
- kathleen - prefers to work asynchronously as well, tough to work with SACM
- (AD) poll the room
- jim s - prefer to do things on the mailing list instead of on phone calls
  - mailing list easier to work with
- adam - phone calls as potential forcing function, but asychronous allows more flexible
- lisa - begging for more feedback on the mailing list
  - (WGC) let's try working group mode for the next few weeks
  - lisa - going to label github issues for easier use
  - lisa - wanting more input
    - document on github
      - put text in github tracker issues
      - edit the document

Information Model
- (WGC) - should we de-emphasize work on info model?
  - lisa - work is progressing, Clif did update
  - adam - please respond to questions on list

Terminology
Henk B
- need to work on the terminology for the loosely coupled architecture changes
  - how to define
    - endpoint
    - capability
- request to (WGC) to provide I2NSF contact for terminology

Plasma for Transport
Jim S
- Does the architecture draft construct a flexible enough arch definition the plasma can be a transport for SACM
- lisa - what is plasma?
- (WGC) *missed the full question*
  - plasma CAN cross enterprise boundaries

- ○ yes out of scope, but it is a possibility
- dave w - is a plasma provider an endpoint or a broker to the endpoint
  - ○ jim s - non sequiter; plasma is a protocol to exchange data
- (WGC) - so plasma is a secure & authenticated protocol that can serve as a sacm transport protocol
- dave w - so plasma is a consumer to provider transport
  - ○ jim s - YES

Way forward
WGC

- good week, progress is made
  - ○ but little conversation on protocols; need more, since protocols is the end game
  - ○ netconf/restconf
- OVAL as possible start for data model

Notes From Danny Haynes

```
=================================================
=================================================
IETF 93
SACM Session I (11:50 PM CEST - 1:20 PM CEST)
July 24, 2015
Prague, Czech Republic
Minute taker #1: Chris Inacio
Minute taker #2: Danny Haynes
Jabber scribe: Jim Schaad


=================================================
Agenda Bashing (Dan Romascanu / Adam Montville)
=================================================
```

[Dan Romascanu]: There was a request over email to allocate some time
on the agenda for the Plasma transport protocol [http://www.ietf.org/
mail-archive/web/sacm/current/msg03124.html]. Time, originally
allocated for the Information Model, was used for this given the
primary focus of the working group over the course of the week was on
the Architecture, Requirements, and Terminology documents.


```
=================================================
Requirements (Lisa Lorenzin)
=================================================
```

[Lisa Lorenzin]: Thanks to Jim and Henk for housekeeping. Now that we
have zero open issues; nine open issues were resolved. Jim proposed
text for the transport protocol. I believe the Requirements document
is now consistent with the Terminology document. Do we want to go
through all nine issues now?

[Dan Romascanu]: Yes, but, go through them quickly for the people that
were not at the meetings.

[Lisa Lorenzin]: Issue #2, #3. With issue #7, there was still some
disagreement, but, Jim Schaad was ready to let go. Jim clarified
issue #36. Issue #48 used data object and improved the definition and
issue #49 was associated with data object.

[Dan Romascanu]: Data attribute designer wondering how we aligned with
the Information Model document terminology. Does anyone have
expertise in this area?

[Kathleen Moriarty]: This came up in the SAAG. The introduction of
terms and how to normalize them. It is not clear what the solution
is, but, maybe we can be the catalyst for this work especially for
data models.

[Dan Romascanu]: Henk Birkholz does the Terminology document.

[Kathleen Moriarty]: I am not sure how this would get solidified (RFC, etc.).

[Dan Romascanu]: I am not sure what would be solidified.

[Kathleen Moriarty]: Again, this is all yet to be determined.

[Lisa Lorenzin]: Yes, we are not trying to duplicate efforts and when we find existing terms, such as those in NEA, we reuse them.

[Lisa Lorenzin]: Next steps. After we go through WGLC, let's not submit the document right away. Rather, let's wait and as we pull in data models and protocols, we can update the Requirements document as we learn more.

[Kathleen Moriarty]: This is definitely a working group decision. In terms of the IESG, you can do this. Of course, you have milestones and those can be amended.

[Jim Schaad]: It may be beneficial to get an AD review.

[Dan Romascanu]: Yes, we can ask any ADs in different groups. It is a pretty low lift.

[Lisa Lorenzin]: I am not sure we are going to make a decision here.

[Dan Romascanu]: Yes, we don't have to.

[Lisa Lorenzin]: To make sure it doesn't get lost, I will send an email to the list with this proposal. The Requirements document was updated last night.

[Dan Romascanu]: We can make WGLC timeline longer than normal.

[Lisa Lorenzin]: I would like to thank everyone for their help over the course of the week.

[Kathleen Moriarty]: It might be more appropriate if the proposal comes from the working group chairs.

==
Architecture (Lisa Lorenzin)
==

[Lisa Lorenzin]: The Architecture document is not as far along, but, we tried to focus on the Requirements document since we are close to finishing it off. There are still fourteen open issues except we are expecting to get more. We have been struggling with the concept of roles (consumer, producer, and controller). We were mixing up terms between capability, functions, etc. Henk Birkholz helped us realize that role is determined by the set of functions. Controller functions are mostly in the control plane whereas the provider/consumer functions were in the data plane. Functions exist in either the control or data plane. Capability is now function and capability is what data models and protocols are supported.

[Dan Romascanu]: With the term capability, we may have created a conflict with the term as used by I2NSF.

[Lisa Lorenzin]: Sorry.

[Dan Romascanu]: Is this an architecture or reference architecture?

[Lisa Lorenzin]: In my experience, reference architecture is an implementation of it. Architecture is just an abstract architecture.

[Dan Romascanu]: I buy it.

[Lisa Lorenzin]: We removed "posture assessment information" from provider and consumer since it is not anything special based on Kathleen Moriarty's comments about information sharing during the Monday session.

[Kathleen Moriarty]: I just wanted to clarify that I was not expecting for you to change the scope of the Requirements document.

[Lisa Lorenzin]: ??

[Kathleen Moriarty]: I think it brings it a little out of scope for the charter. Let's make sure this is known by the working group.

[Adam Montville]: We use GitHub. All of the work is done out in the open. Not in secret.

[Kathleen Moriarty]: I know that, but, people are very busy and don't have time to respond.

[Lisa Lorenzin]: Yes, I think this is more of just a comment.

[Kathleen Moriarty]: I just want to clarify my statement.

[Lisa Lorenzin]: How are we doing for time?

[Dan Romascanu]: You have five minutes.

[Lisa Lorenzin]: We would like people to review the Architecture document. We added a new section explaining what capability is. Looking for feedback on how to think about it in a high-level manner. Is anyone concerned with restructuring? There are additional resolutions that need to be incorporated in the Architecture document. I noticed that we get more done in the room. So, I would like to propose that we have calls for working through these issues.

[Dan Romascanu]: Would you want to follow the working group format (i.e. virtual interim meeting)? Or, would you want to follow the design team format? The working group format is more formal, but, the design team format needs a charter, etc.

[Henk Birkholz]: The Endpoint ID Design Team meetings require two hours which is big commitment.

[Dan Romascanu]: All design teams don't have to be the same.

[Lisa Lorenzin]: I agree. I don't need another two-hour meeting.

[Adam Montville]: I would like to see us work more asynchronously (i.e. not just using phone calls), but, it is up to the working group.

[Kathleen Moriarty]: I would like to see more asynchronous work too because calls can be difficult for people to attend.

[Jim Schaad]: I would like to see more asynchronous work as well. Calls are difficult.

[Adam Montville]: I would like to see more on the mailing list.

[Lisa Lorenzin]: I am fine, but, no one responds.

[Dan Romascanu]: Let's try working synchronously for the first few weeks. Send a list of issues to the list.

[Lisa Lorenzin]: Jim Schaad showed us how to use labels.

[Lisa Lorenzin]: Thanks for helping us decided how to get through this. Nancy Cam-Winget and I are very busy and would like contributions to the Architecture document.

[Adam Montville]: Are you saying that you want textual submissions on GitHub issues?

[Lisa Lorenzin]: Anyway to get it would be great. Thanks for all the help from the group.

[Dan Romascanu]: We decided to skip discussing the Information Model in favor of working on the Requirements document. Are you not making progress?

[Lisa Lorenzin]: The Endpoint ID Design Team is progressing and we have updates that Cliff Kahn made. We are also waiting for feedback.

[Adam Montville]: We also have a thread on the mailing list regarding the Information Model.

[Dan Romascanu]: We are now going to go through the update on the Terminology document.

==
Terminology (Henk Birkholz)
==

[Henk Birkholz]: I would like to apologize that I do not have any slides and thank everyone who helped. The breakout sessions were good. The results of changes from this week are not well represented in the draft Terminology document. They are missing, but, I will update the document. The major task is that we need to define target endpoint and what it is not. Terminology is not strict and across editors we want to have a loose association around containers and attributes of containers. I think this will be in the Information

Model document, but, also in the Terminology document. This is not exclusive to SACM as it may be applicable to other working groups. I would like feedback from the working group. Regarding capability, Dan Romascanu if you could help initiate that conversation with I2NSF that would be great.

[Dan Romascanu]: They are not a working group – just a BOF, but yes, we can get in touch with them.

[Henk Birkholz]: Thanks again with the help. I think things will go smoothly.

```
=================================================
Plasma (Jim Schaad)
=================================================
```

[Jim Schaad]: We may have to make some changes in the Architecture document. I am not saying Plasma should be used in SACM, but, it may at some point. I did this to see if the Architecture document would support Plasma.

[Lisa Lorenzin]: I don't have any context. How do I find out about Plasma?

[Jim Schaad]: Search the IETF site for Plasma. Jim then went over the design of Plasma.

[Dan Romascanu]: What is the red vertical line?

[Jim Schaad]: It means the Consumer and Provider can be inter-organizational.

[Dan Romascanu]: SACM is focused on one organization and one enterprise.

[Jim Schaad]: In the Plasma architecture, the Provider and Controller are working indirect and there is no pre-communication negotiation through the Controller. I would like to see this supported.

[Chris Inacio]: I don't see that this is precluded from the SACM Architecture. I read it as requirements.

[Jim Schaad]: Maybe I was reading it too strictly.

[Chris Inacio]: I guess it is not clear enough.

[Dave Waltermire]: Is a Plasma provider an endpoint or broker to an endpoint?

[Jim Schaad]: It is a protocol. The question doesn't make sense for what the answer is.

[Dan Romascanu]: I didn't read the Plasma document, but, it would be a mechanism for SACM transport?

[Jim Schaad]: Yes, this would be a SACM transport.

[Dave Waltermire]: Is Plasma a Consumer to Provider transport?

[Jim Schaad]: Yes.

[Dan Romascanu]: This was a good week for closing issues and making progress, but, I am worried about not designing protocols. I think at some point in time, we need to start focusing on SACM protocols. We have XMPP-Grid, NETCONF, RESTCONF, and OVAL.

[Adam Montville]: OVAL is a data model. I would add that we probably won't take all of OVAL, but, the pieces that we like.

[Lisa Lorenzin]: Should we map XMPP-Grid to the Requirements document?

[Dan Romascanu]: Let's send it to the second WGLC first.


```
=================================================
Way Forward (Dan Romascanu / Adam Montville)
=================================================
```

[Dan Romascanu]: We need to put the Requirements document through a second WGLC.

[Lisa Lorenzin]: Can you put up the milestones for SACM?

[Dan Romascanu]: We need to avoid serialization where possible. Use GitHub for issues.

[Lisa Lorenzin]: On the last two weeks, the WGLC for the Requirements document should be extended until August 20th.

[Dan Romascanu]: I would also request an early review from the SEC, OPS-DIR, and GenArt ADs. The new Requirements document should be ready for September 5th. There are lots of open issues for the Architecture document. We should have comments on GitHub for the Architecture document on August 20th. We should then have an Internet-Draft revision on September 12th.

[Lisa Lorenzin]: I don't think the Architecture I-D will be ready for WGLC.

[Dan Romascanu]: We should have a SACM Virtual Interim Meeting during the week of September 12th or September 19th. Also, just a reminder, the I-D cutoff date for IETF 94 is October 19th. IETF 94 is in November.

[Lisa Lorenzin]: I think we will have a bunch of open issues during meetings. I think a realistic timeline for the Information Model document is the end of the year.

[Kathleen Moriarty]: This needs to be changed based on the entire working group. I also just want to clarify that they will not be changed on the fly.

[Dave Waltermire]: I just wanted to call out because there are other editors.

[Adam Montville]: I am frustrated about re-doing milestones and the lack of progress.

[Lisa Lorenzin]: I would like to have a discussion about the Requirements going to the IESG.

[Kathleen Moriarty]: With my AD hat on, I just want to make clear that this needs to go out on the list for review.

[Lisa Lorenzin]: If the working group does not think this is aggressive enough, what happens?

[Kathleen Moriarty]: This generates discussion to reach consensus.

[Adam Montville]: Thank you.

[Dan Romascanu]: Děkuji (thank you in Czech).