Back to the wiki for this working group

Federation Interoperability Working Group Scribing Document

NOTE WELL: All Internet2 Activities are governed by the Internet2 Intellectual Property Framework. https://www.internet2.edu/policies/internet2-intellectual-property-policy/

Coordinates: 10 a.m. ET each Monday

Dial-in:
+1-734-615-7474 (English I2, Please use if you do not pay for Long Distance), +1-866-411-0013 (English I2, toll free US/Canada Only)
Access codes:
0143080 (Participant)

Agenda - 1/8/2016

- Europe
  -
- Eastern Time Zone
  - Tom Scavo (InCommon)
  - Scott Cantor (OSU)
- Central Time Zone
  - Walter Hoehn (Memphis)
  - Barry Ribbeck (Rice)
  - Brett Bieber (Nebraska)
  - Mike Grady, Unicon
- Mountain Time Zone
  -
- Pacific Time Zone
  -
- Other

Agenda:

- Review Strawman Final Report
  - https://docs.google.com/document/d/1zNHpOith2r6E_RMPGRDd3wIfcdzk1hSzLXPX6JT6qXw/edit?usp=sharing
- Call for Profile Review went out on Jan 26. Review will end on Feb 15
  - Announcement sent to numerous mailing lists plus Ellucian and Microsoft
  - Tom AI: Send copy of announcement to simpleSAMLphp mailing list

Agenda - 1/25/2016

- Europe
    -
- Eastern Time Zone
    - Scott Cantor (OSU, Shibboleth Consortium)
    - Tom Scavo (Internet2/InCommon, Ann Arbor)
- Central Time Zone
    - Walter Hoehn (Memphis)
    - Barry Ribbeck (Rice)
    - Brett Bieber (Nebraska)
- Mountain Time Zone
    - Nick Roy (I2/InCommon)
- Pacific Time Zone
    - Judith Bush (OCLC)
    - Eric Goodman (University of California)
- Other

Agenda:

- Path Forward: Charter vs. Timeline, etc.
    - How to proceed when the profile is complete
    - List/off-list discussion
    - Syncing up with the group
    - Original charter from TAC was very broad, timeframe to wrap up was end of December - typical timeframe is 4-5 months
    - How to proceed with work we have not gotten to so far?
        - Request extension?
        - Report to TAC now? List outstanding items in report, possibly recommend spinning up a new group to address outstanding items
        - Often, the charters are ambitous, this WG charter certainly is
            - In past, WG goes to TAC, TAC accepts work products, re-charters new group with charter that includes a mix of old/new items discovered or uncompleted. This is not unusual.
        - Next steps:
            - Deployment profile (saml2int) (couple options for doing this, either in InCommon as recommendations to Kantara, or direct people to Kantara WG-FI)
            - Set of guidelines/other stuff - won't know specifics until we go through the exercise of drafting the report.
        - Walter likes the idea of wrapping up in roughly the timeframe that was asked of us, and present back with something that is complete/good. Not

opposed to continue to help with whatever is ongoing. A lot of what needs to get done is probably best pushed over to Kantara.
        - Preferences: Wrap up this group, move to Kantara
        - Concern: Might not get people to show up to that group, or might not be able to have focus on the use cases for our community, if we don't start outside that group, identity what's unique for us, and push it into Kantara.
        - ScottK would likely agree - some amount of InCommon and research-specific recommendations we could offer, we've discussed quite a bit but put them off as a deployment thing.
    - ***No objections on the call*** to wrapping up the group and recommending the TAC re-charter or hand-off for the next items in the original charter. Allow TAC to weigh in on remaining questions.
    - **AI: Nick write strawman report to TAC, send to the group for editing**
        - **Deployment corollaries exist for many of the items in this profile, plus items from the issues list.**
- Final Review:
    - IIP-G02 (clock skew) - Recommend adding time sync with time servers to a deployment profile
        - **AI: Walter** fix to en-dash between '3' and '5' in clock skew minutes
    - IIP-SP10
        - Question from Judith on why this would not be part of the profile
        - Deployment profile side of this is much harder to nail down - understanding why people can't do things for legitimate reasons. There will likely be legitimate issues in many cases that people haven't considered. Don't even know how you'd craft a deployment requirement around this because it's an artifact of the design and intent of the app. Issue of people confusing the resource URL and the SAML endpoint, which are not required to be the same thing. Should we add a non-normative sentence to that effect?
        - Tom has noted that there are tons of SPs in the federation that don't do this. Why would we require? Answer from Scott: there are a lot of SPs that are broken, and this is an implementation requirement
        - TomS: No strong concerns any more. Am OK with how this is.
    - Metadata-based Configuration
        - IIP-SSO05 (peer configuration via supported metadata elements)
            - **AI Walter:** remove extra 'that' in last sentence: " *configuration that that cannot "*
            - **AI Walter:** First non-normative paragraph, reference to XML element that needs format change (md:AttributeProfile)
            - Group OK with this
        - [IIP-IDP??]:: Implementations MUST support the consumption of peer configuration values from SAML metadata, without additional inputs or

separate configuration, for any element listed in the "Use of Metadata" section for the Single Logout Profile in <<SAML2Prof>> (section 4.4.5).
                - Group OK with this
            - [IIP-IDP??]:: Implementations MUST support the consumption of peer configuration values from SAML metadata, without additional inputs or separate configuration, for any element listed in the "Use of Metadata" section for the Enhanced Client or Proxy (ECP) Profile in <<SAML2Errata>> (section E20).
                - **AI Walter:** look at reference, should it be to ECP 2?
                - Group OK with this
            - [IIP-IDP13]
                - **AI Walter:** Replace errant parenthesis from last sentence with period.
            - 4.1.6 vs 4.1.7
                - Meta comment: would be great if we could get the docs that are only referenceable/usable via errata updated to include the errata in a new rev.
    - IIP-SP13
        - Rainer +1'd this via email
        - Group OK with this
        - Deployment profile should capture something about requirements around minimal POST size to handle (**AI: whoever submitted this**: Add to interop issues list)
- Verify names in contributors section
    - Eric notes: There should be a comma after "California" in my location. (**AI Walter:** Fix) i.e., "University of California, Office of the President" (ooh… note that I also lower-cased "the" in "of the")
    - Brett requests: University of Nebraska-Lincoln (**AI Walter:** Fix)
    - Judith requests "Judith E Bush" (**AI Walter**: Fix)
- Review period: 3 weeks, on lists, TAC would like InCommon Participants and REFEDS
    - Tentative plan: Walter to open document for review on Wednesday's IAM Online.
    - Scott expressed some concern about how well we will be able to scope people's comments to implementation vs. deployment profiles.
    - Judith could present at IIW in April 26-28
- **AI Walter:** Spelling correction, section 1.1 'requirments' (in second to last sentence of the section)
- Scott: this is actually a really good way for the OpenID crowd to be able to understand our needs in this space.

Agenda - 1/11/2016

- Europe
    -

- Eastern Time Zone
    - Scott Cantor
    - Tom Scavo
- Central Time Zone
    - Walter Hoehn (Memphis)
    - Mike Grady (Unicon)
    - Brett Bieber (U of Nebraska-Lincoln)
- Mountain Time Zone
    -
- Pacific Time Zone
    - Eric Goodman
    - Judith Bush (OCLC)
- Other
    -

Agenda:

- Final Review:
    - IIP-SP09
        - Second non-normative note should refer to the (apparently missing) normative requirement to read endpoints from metadata
        - Should remove the specific erroneous approach. I.e.:
            - *Note that discovery mechanisms should determine the endpoint(s) to which requests are to be issued via SAML metadata ~~and not by hardcoding links to specific endpoints~~.*
    - IIP-G02
        - 2.2 section was renamed from NameID->General
        - Discussion focused on whether the list of extensions should be listed as complete. Recommendation to change the language to say something along the lines of “A non-exhaustive list…”
        - **AI: Scott** The non-exhaustive list should be moved to the non-normative text.

- We noted that the text that follows was missing from the document:
    - Implementations must be capable of interoperating (leading to success or failure as dictated by policy) with any number of SAML peers for which metadata is supplied, without additional inputs or separate configuration. Metadata alone MUST be sufficient to provision a peer to interoperate in accordance with the default configuration of the software. Each SAML profile defined in [SAML2Prof] has a section describing how metadata is used to achieve this interoperability; recommendations (SHOULDs) these sections (4.1.7, 4.2.6, 4.4.5, 4.5.5, 5.5, 6.5, 7.5) are to be interpreted as normative requirements of each profile, rather than optional features as originally specified.

- Proposal from Eric:

When specific constraints are absent in the SAML standards or profile documents, all XML **xs:string** type ~~NameID and AttributeValue~~ elements and attributes MUST be able to accept values containing a minimum of 256 characters, comprised of any combination of valid XML characters without error or truncation. This requirement applies both to types defined within the SAML standards (such as transient and persistent NameIDs) and to types defined by the user within an implementation.

It is acceptable to allow users to selectively configure more restrictive constraints on specific NameID and AttributeValue type

- Proposal from Rainer:

  [IIP-SP11]:: _It is recommended that SPs preserve the client's request state when a request requires re-authentication after a timed-out session. This pertains to URLs (example: "deep linking") and POST form data ("POST preservation"). Implementations may choose client- or server-side storage depending on typical requirements. While this recommendation is not specific to SAML Web SSO, adhering to it can prevent very unpleasant user experiences (example: session expires while user is editing a web form, user submits web form, content of submission is lost due to expired session and need to redirect to the IdP for re-establishment of the session)._

- Proposal from Scott:

  -[IIP-MD03]:: Implementations MUST support the interpretation and application of metadata as defined by the SAML V2.0 Metadata Interoperability Profile <<SAML2MDIOP>>. Support for other metadata profiles is OPTIONAL. It follows that implementations MUST be capable of interoperating (leading to success or failure as dictated by policy) with any number of SAML peers for which metadata is supplied, without additional inputs or separate configuration. That is, metadata alone MUST be sufficient to provision a peer to interoperate securely in accordance with the default configuration of the software. In accordance with the SAML V2.0 Metadata Interoperability Profile <<SAML2MDIOP>>, metadata MUST be:

  +[IIP-MD03]:: Implementations MUST support the interpretation and application of metadata as defined by the SAML V2.0 Metadata Interoperability Profile <<SAML2MDIOP>>. Support for other metadata profiles is OPTIONAL. It follows that implementations MUST be capable of interoperating (leading to success or failure as dictated by default configuration) with any number of SAML peers for which metadata is supplied, without additional inputs or separate configuration. In accordance with the SAML V2.0 Metadata Interoperability Profile <<SAML2MDIOP>>, metadata MUST be:

  and later…

  +_Note that this requirement does not preclude supporting a variety of configuration options on a per-peer (or other) basis; it simply requires that default behavior be possible without such._

  - Discussion: Concern about the ambiguous nature of “default”.
  - We edited the requirement to put the term “default configuration” inside the parens, removed the word “policy”

- Proposal from Scott:

  +[IIP-SP11]:: Implementations MUST support deep linking. That is, it MUST be possible to access an arbitrary protected resource and (authorization permitting) supply that resource as the result of a successful SAML response. Support for unsolicited responses (or so-called IdP-initiated SSO) is NOT a substitute for this capability.

- Proposal From Scott:

  +[IIP-SP10]:: Implementations MUST support the processing of responses from any number of issuing IdPs for any given resource URL. That is, it MUST NOT be a requirement of an implementation that support for multiple IdPs require non-uniform resource URLs. The previous requirement for support of <<IdPDisco>> leads naturally to the elimination of this restriction.

  (Should last sentence be moved into non-normative text?)

Agenda - 12/21/2015

- Europe
  - Rainer Hoerbe (Kantara)
- Eastern Time Zone
  - Scott Cantor (OSU, Shibboleth Consortium)
- Central Time Zone
  - Walter Hoehn (Memphis)
  - Paul Caskey, Internet2
  - Mike Grady, Unicon
  - Brett Bieber, Nebraska
- Mountain Time Zone
  -
- Pacific Time Zone
  - Eric Goodman (University of California)
- Other
  -

Agenda:

- Clock Skew
- IIP-SP09 - Unsolicited Requests
- IIP-MD03 - To what does this apply?
  - Agreement that language should be added to clarify that we're talking about non-trust metadata as well as trust-based metadata.
  - Discussion of how to call this out

    - Scott: Do we want to note that apps can still use manual per-entity config so long as config via metadata is acceptable?
    - Rainer: it should be possible to add a new entity without requiring in-app configuration.
    - Scott notes that the lack of an MDIOP section in the metadata is not an indication that metadata is NOT supported.
        - Rainer: Do we need language to address the case of lack of a MDIOP section?
    - Scott, Walter: Preferred direction is to call out that we are not precluding support for in-app, per-entity configuration, even though metadata must be consumable and sufficient.
    - **AI: Scott** to propose wording about ability to do in-app per-entity configuration and addressing the fact that lack of metadata does not mean “you may not support this”
    - **AI: Scott** will also propose some of the specific metadata use cases that might be worth specifying, such as not using nameid profiles that are listed
    - **AI: Walter** to propose wording (or a new requirement) to clarify the breadth of metadata support required, possibly “it should be possible to add a new entity without requiring in-app configuration”.
- Multi-IdP Support - single URL access question
    - **AI: Scott C**; new “protect the URL” SP requirement
    - Addressed by 3 items:
        - MD03 or new “any number of SAML peers”
        - Discovery service
        - New SP10 talking about protecting resource URLs
- Open issues
    - Support for deep linking
    - Step up authentication?
- Public Review
    - when: early next year, but we do need an additional call then
    - how long: upper bound one month
    - who: InCommon participants. Kantara? (would require added IPR text, too)

Agenda - 12/7/2015

- Europe
    - Rainer Hörbe (Kantara)
- Eastern Time Zone
    - Scott Cantor (OSU, Shibboleth Consortium)
    - Tom Scavo (InCommon)
- Central Time Zone
    - Walter Hoehn (Memphis)
    - Brett Bieber (Nebraska)

    - Barry Ribbeck (Rice)
    - Tommy Doan (Southern Methodist University)
    - Scott Koranda (late, LIGO and SCG)
- Mountain Time Zone
    - Nick Roy (I2/InCommon)
- Pacific Time Zone
    - Eric Goodman (University of California)
- Other
    -

Agenda:

- Note Taker: Nick Roy
- Welcome
- Discussion re: Wrapping Up the Draft
    - TomS: Looking pretty good
    - Any reasons we wouldn't be able to get outstanding items fixed within the next week?
    - Scott: Will try to wrap up the metadata requirement with extensive discussion, but don't know how far will get.
    - Walter will be on TAC call on Thursday to give them a heads up that's coming, and get advice on who to reach out to for next steps/final review.
- Outstanding Issues:
    - IIP-ALG04/05 - discuss on Monday - these seem to require SP decryption, which was purposefully left out of other sections. Question: Are we sure we don't want to require decryption at the SP, and do we want to adjust this section?
        - ScottC: I think we absolutely want to require SP decryption
        - Rainer: Should we limit that to assertions and encrypted IDs?
            - ScottC: I thought we had limited it to those
            - Walter: Outside of the ALG section, there is nothing that says the SP has to decrypt. That needs to be fixed.
            - ScottC: The IdP half is still there IIP-IDP12
            - Walter: On a practical level, if you get past the metadata requirements, which is the heart of the spec, encrypting by default and having it break is high up on the list of problems to solve.
            - The problem: There is no SP requirement that corresponds to IIP-IDP12
            - TomS: Need to make clear that the SP needs to support two encryption public keys in metadata on the IdP side to allow key rollover
            - Walter: Propose we add a new requirement somewhere in the SP section that explicitly says that decryption is required, and limited to decrypting assertions and encrypted IDs

- Scott: IIP-IDP18 has not been settled, this needs to get settled since it will have a ripple effect through requirements on both roles
- TomS: IIP-MD08 needs to be a software requirement, not a metadata requirement.
- Walter: Not opposed to moving it, but it goes together with the requirement before it.
- TomS: The previous two go together, not MD08. MD08 IS the decryption requirement at the SP, those words exactly. Need to make a decision on IDP18 first to determine where MD08 should go.

- IIP-IDP18 - Keep it in or not? How to bundle that with the above item?
  - Walter: Not a good sense about whether there is consensus on this item
  - TomS: This could be needed in the future, and if we don't include it in this document then we lose the window of opportunity.
  - ScottC: Logout in general is going to cause you more pain than decryption. Want to defer to Rainer, will this be a point of contention if we take this out.
  - Rainer: Know of some government IdPs that have this in their requirements, **would keep IDP18 for that reason.**
  - ScottC: This was part of the base conformance specs, we're not imposing something new.
  - Walter: Any objection to leaving IDP18
  - **AI Walter:** Will fix this up
- IIP-MD08 - SP decryption requirements
  - ScottC: This can now go in the IdP's Browser SSO section and SP's SLO section. You could also add this as a supplemental section to IDP-18 and the SP section, change the first clause. When you test for encryption inbound, you can test that it works, and test for support for two keys at the same time.
  - **AI Walter:** Move into IIP-IDP18, and move to SP Web SSO.
- IIP-SP05 - AI: Scott will suggest text - clarify "simple element content"
- Issues List 9 - AI: Walter will suggest text
  - Walter: Consensus on the list was that we should quote the errata and include in Common Errors.
  - Brett: Time synchronization is something that gets run into constantly, beyond just clock skew.
  - Walter: Point well taken, but this is probably in a lower layer, not in SAML implementation. Doesn't hurt to say it, can possibly/probably park for SAML2int. Could make it a non-normative note in the current document.
  - **AI Walter:** Will come up with text for this
- IIP-IDP14 - need to decide whether to include GSS-API text
  - **AI Scott:** Will send it to the list
- IIP-IDP17 - need to decide whether to include requirement, Kantara Gov?

- IIP-MSG04 - AI: Scott will suggest clarified text
  - ScottC: Not sure what this got renumbered to.
  - Brett: In notes from Nov 23rd
  - Walter: “Implementations must support signing of both the response and assertion layers”
  - ScottC: Appears to have been removed
  - Eric: It’s now IIP-SSO04 (common requirement)
  - ScottC: Having these four requirements as common requirements will confuse people.
  - **AI Walter:** Will help Scott out with writing the revised ECP and SSO common requirements. Will do this on chat or something. (This is the last to-do below)
- IIP - CE01/Issues List 14 - AI: Both Eric and Scott - needs to be moved into MD section, normative vs non-normative text cleanup, clarification re: Issues List 14 - further work should take into account Eric’s 11/24 suggested text on list
- IIP-IDP05/06 - discuss on Monday - MUST, SHOULD, or delete
  - TomS: MDRPI is definitely getting used in eduGAIN
  - Not sure if this will be widely used by deployers for attribute release decisions.
  - Nick: Policy use cases could support inclusion
  - ScottC: Predict that eventually rpi stuff disappears, shouldn’t be used for attribute release decision making.
  - Walter: Opinion is it’s not useful, haven’t seen many use cases
  - Nick: Scott makes a pretty compelling case for not using it, I’d be OK with deleting it.
  - Brett: Feel like mdrpi is what we should be using to make interfederation policy decisions
  - ScottC: That’s not currently being done in an appropriate way by the eduGAIN profile. If you wanted to do that in the right way, you should be using entity attributes
  - TomS: MDRPI isn’t the best place to call out the policy you’re interested in, the entity attributes are. In fact, have already done that in the case of the InCommon registration authority (registered-by-incommon category)
  - Brett: If MDRPI is not the right place, should we make a recommendation on entity attributes?
  - Nick: Probably not in this implementation document, but could add it to the issues list.
  - Walter: Consensus is that we should remove this
  - **AI Walter:** Pull this out, and renumber all of the subsequent things
- IIP-IDP07
  - Nick: This one is a really common practice in other federations.
  - TomS: That’s a good point, and happy with this one the way it is
  - Walter: Anyone differ?

        - Meta attribute discussion: Leif was pushing that, thought it would emerge in REFEDS. If you don't do this, requested attributes are just useless. In terms of writing a requirements in this implementation profile, not sure how would write that.
        - Meta attributes required to make this useful, but that is probably not documentable in this profile at the current time.
    - IIP-IDP14 - WFH/SC - fix references

Agenda - 11/30/2015

- Europe
    -
- Eastern Time Zone
    -
- Central Time Zone
    - Walter Hoehn (Memphis)
    - Brett Bieber (University of Nebraska-Lincoln)
    - Mike Grady (Unicon)
- Mountain Time Zone
    -
- Pacific Time Zone
    - Eric Goodman (University of California)
- Other
    -

Agenda:

- Note Taker: Eric Goodman
- Welcome
- Agenda Bash
- Discussion: Interop Issues Matrix (Eric)
    - Eric gave an overview of what the page was
        - Issues were pulled from emails prior to the initial group meeting, where participants called out what was problematic in vendor implementations.
        - Mapping of issues to needed requirements was done by Eric, not reporters of issues
        - Other columns indicate whether requirement is addressed and where in the document it is addressed based on Eric's review (at least prior to the discussion at this meeting).
    - *Issue 14* (SPs must interop with multiple IdPs)
        - Is this addressed by covered by the MD and discovery service requirements
        - Mike: Does discovery requirement (SP08) cover this
        - Brett: Agrees that it should be called out specifically.

        - **AI: Eric** Take an AI to update an existing requirement (MD11 and/or SP08) with non-normative information and/or add a new requirement to address it.
        - Discuss was whether MD11 makes it clear that consuming metadata implies that they can interoperate with more than one IdP (accept assertions from more than one)
    - *Issue 16 (literal account IDs in IdP)*
        - Walter thinks this is addressed in SP02
        - Eric: looks more like an issue about what data is required in the nameid (that the IdP must maintain internal SP IDs)
        - Agreed that one of the underlying requirements is addressed in SP02, and that is probably the best we can do
    - *Issue 9 (clockskew)*
        - This is part of the SAML spec (at least in errata), so that may be why we didn't include.
        - Should we add at least an "avoid common errors" item?
        - Question as to whether this was an issue for IdPs or just SPs. Agree it's just a general requirement.
        - Should perhaps call out that the implementation should be able to allow configuration of the amount of clockskew allowed?
        - **AI: Walter?** Add an item to address this.
        - Probably should be noted or referenced in MD05 (validity periods) as well
    - *Issue 10 (Support for XML encryption at the SP)*
        - Section 2.5 calls out encryption requirements
        - SSO04 calls out signing
        - IDP11 calls out encryption
        - There is no requirement in the SP that calls out SP encryption is required. So existence of IDP11 makes section 2.5 [lost the thought…]
        - MD08 (key rollover) strongly implies that inbound SP encryption is optional (*"If an implementation supports inbound encryption"*)
        - **NOT ADDRESSED**
        - **AI: Eric** raise this issue on the list
    - *Issue 19 (Step up authentication)*
        - Is there an implementation aspect of this requirement?
            - Yes, we agree that this has implementation implications.
        - Is this something that the implementation should support?
        - Ran out of time on the call during discussion of this item
        - **AI: Mike** will raise this issue on the list.
    - **AI: Eric** to update issues list to capture discussion noted above.
- Next Steps/Time Frame: Implementation Profile
- Outstanding Issues
    - IIP-MD10/IIP-SP01/IIP-IDP01 (WFH)

        - Concern is whether these elements agree. In MD10, there are different requirements for IdP vs SPs in one requirement element. Vs. SP01 and IDP01 which are the same kind of separate requirement {MUST for IdP, SHOULD for SP) but are split into two requirements.
        - In discussion there was agreement that it should be split.
        - **AI:** Walter will update as a split.
    - IIP-IDP04,IIP-IDP05,IIP-IDP05,IIP-IDP06 (MUST/SHOULD) (Tom S.)
    - IIP-MD07,IIP-MD08, IIP-IDP17 (IDPvsSPvsBoth, where is encryption required) (TomS/Scott C.)

Agenda - 11/23/2015

- Europe
    -
- Eastern Time Zone
    - Scott Cantor (OSU, Shibboleth Consortium)
- Central Time Zone
    - Walter Hoehn (Memphis)
    - Scott Koranda (SCG and LIGO)
    - Tom Scavo (InCommon/Internet2)
    - Tommy Doan (Southern Methodist University)
    - Barry Ribbeck (Rice)
- Mountain Time Zone
    - Nick Roy (InCommon/Internet2)
    - Nate Klingenstein (Internet2)
- Pacific Time Zone
    - Judith Bush (OCLC)
    - Eric Goodman (University of California)
- Other
    -

Agenda:

- Note Taker: Nick Roy
- Welcome
- Agenda Bash
- Outstanding Issues
    - ECP
        - Section 3.4.2
        - Question: Do we want to require features required for support of GSS-API?
            - Scott C inclined to say we should - it's pretty easy to do
            - Eric: what does that give you?

        - IdP's ECP support can be used to support the GSS-API work that Clemson is doing
        - **AI Scott:** will send summary of what's needed to the list
- Logout
    - Section 3.4.3
    - Tom S: First sentence of IIP-IDP15 should be broken into two sentences
    - **AI Tom S:** Will propose a change to resolve, and send to the list
    - Question: Should we keep IIP-IDP17? (Support for EncryptedID in logouts)
        - Scott C leans toward not requiring it but thinks we have to
        - Reasoning: If you use anything other than transientID, it's not great to have cleartext IDs sitting in web server logs
        - Reason don't like this is encryption is a big deal, this is an entirely new requirement that adds a lot of complexity to implementations. Needs to have a keypair to do the encryption/decryption, that keypair needs to be managed, etc. Not something that can be done lightly
        - This why they did transientID to begin with, but unfortunately the most interoperable/common use of nameID will be persistent
        - Walter: need to think on this more to have an opinion
        - **AI Scott C:** Will take a look at Kantara eGov profile to see what is done w/r/t this there
            - (line 293 or so)
            - "Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the <saml2:EncryptedAssertion> element when using the HTTP-POST binding; support for the <saml2:EncryptedID> and <saml2:EncryptedAttribute> elements is OPTIONAL."
            - (line 388 or so)
            - "Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the <saml2:EncryptedID> element when using the HTTP-Redirect binding."
- SP Attributes
    - Section 2.3
    - Walter happy with IIP-SP03
    - Scott C recommends it to be retroactively compatible with IIP-SP05
    - **AI Walter:** Will do that
    - Discussion of the "must gracefully drop attributes they don't understand" language - fits where it is, doesn't fit in common errors section.
    - **AI Walter:** will pull into a separate requirement for granularity of testing
    - IIP-SP04 - seems pretty clear, not sure how testable it is
    - IIP-SP05 - What does simple element content mean?

        - **AI Scott C:** Will clarify that
        - **AI Nick:** Will correct nit on second sentence “implementation” → “Implementations” (fixed)
    - Section 2.4.1
        - IIP-MSG04
        - Don’t know how to word to make it clearer, that you don’t have to sign both layers
        - Should be moved under common errors? It’s been modified by errata countless times to try to prevent the error of interpretation that both layers don’t need to be signed.
        - **AI Scott:** Will try to make it clearer in the document
    - Encryption
    - Section [2.1.5, 3.1.5]
        - IIP-CE01
        - Proposal to add the stuff at the end, change first sentence, Walter responded with a couple updates including making last part non-normative
        - Could live with the last part (example) being non-normative if there is an explicit mention of TLS in the normative part of the requirement. This is virtually every TLS library in existence. If you don’t say it, you’re not going to get it. Needs to be normative or we need to preclude TLS.
        - Could we break it up to require TLS and behavior in the way we need, but talk about TLS libraries in the non-normative text?
        - Scott C AI: Will write TLS requirement into the normative part of the text (another half sentence with quote from MDIOP that is explicit about this)
        - Eric AI: Will write another non-normative example of behavior that’s needed
        - This was originally in one of the top tier metadata sections, then Walter added reference to MDIOP with the direct quote, but if we’re quoting other specs should this be our own requirement or in common errors?
        - **Scott C AI:** will do something towards the top of the document to highlight that the metadata you’re consuming is aligned to this particular profile.
- Encryption section re-import from Rainer’s doc
    - There are currently no common sections
    - This would introduce one
    - There are multiple sections that could be common if we have a common section
    - We should either do it or not do it
    - Arguments against doing what we’re doing right now is that it makes it seem longer than it is
    - Scott C strongly prefers the common section approach
    - Walter - would be a big change to pull things out and reorganize to have a common section

    - Would probably end up with about 2/3 of the document in the common section, have to be an IdP and SP specific sections, would replicate the structure of the common section
    - The choice is split it into two separate documents, or keep it a single document and do a common section.
    - Duplicating content leads to confusion in the long run
    - Proposal: separate document into three sections:
        - 1) All common material
        - 2) IdP specific section
        - 3) SP specific section
        - Common material would include the algorithm stuff
        - Probably the IdP and SP specific sections have to mirror the outline of the common section. Example: Look under service provider, section 2.1: within 2.1.2 is an SP-specific requirement. So in the SP-specific section, you're going to want to have SP-specific metadata requirements section.
        - 2.3 is another good example - all of the requirements are either SP-only or IdP-only
    - **Walter AI:** Willing to do this work but want to be confident that this is what the group wants. Hearing nothing but support for this - speak now or forever hold your peace.
- Issues Matrix
- Plan Moving Forward
- Document Hosting during eval period
    - Questions for TAC?
        - Should the profile be split up into SP and IdP docs, or single doc?
- **AI All:** Read through the whole document after restructuring, make sure it makes sense.

Agenda - 11/2/2015

- Europe
    - Rainer Hörbe
- Eastern Time Zone
    - Scott Cantor (OSU, Shibboleth Consortium)
    -
- Central Time Zone
    - Walter Hoehn (Memphis)
    - Barry Ribbeck (Rice)
    - Paul Caskey (Internet2)
- Mountain Time Zone
    - Nick Roy (Internet2)
    - Nate Klingenstein (Internet2)
- Pacific Time Zone
    - Judith Bush (OCLC)

- Other
    -

Agenda:

- Note Taker: Nick
- Welcome
- Agenda Bash
- Discuss Rainer's Draft Algorithm Spec
    - https://github.com/KantaraInitiative/SAMLprofiles/blob/master/docs/SAML%20Algorithms/Algorithm_Support.adoc
- Review of Several Items:
    - IIP-SP04
    - IIP-IDP02
    - IIP-EXT01
    - IIP-SP02

- Rendered: Rendered Snapshot
    - Source: ADoc Source

- Notes
    - Rainer's Algorithm document: contents/how it might be handled in Kantara/timeframe/how to reference
        - Step 1: Propose this document as an official document on the next Kantara call (Kantara interop group?)
        - Step 2: Will be able to feed back a plan to this group based on the outcome of the Kantara discussion
        - Question: should we keep this in Kantara, or go to IETF?
        - ScottC: If you go the IETF route it may be more contentious
        - Walter: Wanted a small section we could link to that had a more lightweight process for updating it. Something standalone that we could easily update/sunset/etc.
        - Rainer agrees - this would point toward keeping it in Kantara
        - Scott - intuition is that the only way to make it beneficial is if it's maintained on some regular interval and has to be revisited every year or every other year, so there is a cycle to it. Guidance that's kept up-to-date. Otherwise, it wouldn't be much different than if it's in the implementation profile document.
        - Our spec could say, "you should have current year or last year's version in effect at any time."
        - Rainer: Question: can it be done very lightweight via putting it on the agenda of the interop WG in Kantara, or does it have to go by the Kantara assurance review board?

- Scott: There's a danger to assuming that because the last few years have been a nightmare w/r/t security, the next few years will be too. We've probably seen most of the transitions we're going to see, with the exception of the RSA to ECDSA transition.
- Judith: SURFnet is asking that you get a grade at the Qualys SSL Labs test. They say they won't connect you their hub unless you get a certain grade. That's for front channel, not signing.
- ScottC: Probably don't want to go into TLS in this document, would need another section.
- Judith: But, it came to mind because what Qualys is doing is a continual assessment of "what is an 'A'?"
- Rainer: That's why the inclusion of bettercrypto.org. For TLS, included in requirement #5, and link to bettercrypto.org. Applies to front and back channel, wherever you require TLS. Would keep TLS requirements non-normative, because it's a huge amount of work.
- ScottC: It may be that the answer is to actively go in the direction of message-level encryption instead of using TLS as part of this spec. Otherwise, we have to think about when/how to jump to TLS 1.2. Have taken some baby steps in that direction - IdPv3 treats TLS connection over 443 as insecure. So turn on signing and encryption by default. Need to do the same thing on the SP side. For the purposes of this conversation, we have to either:
    - 1) be specific about TLS requirements
    - 2) OR make a definitive statement about moving off the TLS layer for crypto
- Rainer: I would refrain from making it a MUST.
- Scott: Simpler thing is to move off the back channel and move off use of TLS for the back channel.
- Rainer: For time being, for everyone who still relies on TLS, make a recommendation.
- ScottC: More comfortable with doing that if we have more concrete guidance on message-level encryption.
- Rainer: Would need some careful wording for that.
- ScottC: We're not mandating anything that's specifically backchannel. Only going to mandate front-channel log out.
- Discussed CBC mode in Cleveland - for interoperability, not for security. That would be the sort of thing where the goal would be to move to GCM. That point with regard to those algorithms would be worth having a sentence about.
- Rainer: Would be good to have a template companion document in Kantara that could be used for other profiles.
- ScottC: Put a header at the top of the Algo document "The following algorithms are being included for the purposes of interoperability and

backwards compatibility and will be removed in a future version of this document."

- Walter: For linking into the Interop Profile, should we link directly from the individual requirements that have a dependency on it, or link to an internal section that links out to the Algo spec?
- Nick: Could still direct link to the Algo spec from the individual requirements, but have a non-normative note about updates to the Algorithms spec and you should stay up-to-date and that spec refreshes (annually?)
- Walter: Need to call out that the algorithms document is a living document
- Scott: This is the reason that they aren't separate documents today, across the board, the vendors refuse because they have to get compliant and stay compliant, and shifting algorithm specs can't be supported. If you're not going to reference this Algo spec from other documents, it's not worth separating. You're going to have to rev the Interop profile every time you update algorithms, or vendors aren't going to implement. We're beholden to the same technology stacks that everyone else is (programming framework dependent).
- Nick: Should we then, considering that the algorithms are likely to be more static in the near future, just pull this back in?
- Scott: That's what I've gone through every other time we've tried to separate the security algorithms out. The profile itself should be the living document, if for nothing else than the cryptography.
- Rainer: Conformance shouldn't be part of the Interop document, there should be a separate conformance document
- Scott: The Interop profile is a conformance profile.
- Walter: Let's take it as a given that we all agree on fact that if we have to rev our document for crypto, are there other reasons for not pulling the algorithms back in?
- Scott: Don't see a hugely compelling advantage to keeping these separate. The eventual deployment profile is really just profiling down this single document. Makes it easier to do that other document.
- Walter: Any objections to pulling it back in?
    - No
- Scott/Rainer: The Algorithm section should be a separate section that applies to both IdP/SP.
- Walter: Let's keep that as a separate question.
- Rainer: Will InCommon provide the regular maintenance, or should the whole thing go to Kantara?
- Scott: I think the whole thing should go to Kantara.
- Nick: Me as well
- Scott: This, specifically, is an area where wider industry input is pretty valuable as well.

        - **Walter Al**: Will pull the algorithm section back in, and will pull it from Rainer's newer version to make sure the new text gets transferred forward. Will think about this issue of how it should be integrated and will propose something on the list.
    - Review of other items:
        - IIP-SP04, 2.4.1: Look OK?
            - **Walter Al**: Update to latest text - SAML metadata is supposed to be removed, and non-normative note has been added. Walter will check it out.
        - Other items: Also out of date. Looks like Walter needs to fix his update script. Will discuss on next call.
    - ScottC: Will finish logout support in new IdP version, will have to push out his tasks for a couple weeks.
    - Other item review: **Walter Al**: will take it to the list.

Agenda - 10/26/2015

- Europe
    -
- Eastern Time Zone
    - Scott Cantor (OSU, Shibboleth Consortium)
    - Tom Scavo (InCommon/Internet2)
- Central Time Zone
    - Walter Hoehn (Memphis)
    - Tommy Doan (Southern Methodist University)
    - Brett Bieber (University of Nebraska-Lincoln)
- Mountain Time Zone
    - Nick Roy (Internet2)
    - Nate Klingenstein (Internet2)
- Pacific Time Zone
    - Judith Bush (OCLC)
- Other
    -

Agenda:

- Note Taker: Nick Roy
- Welcome
- Agenda Bash
- Discuss Rainer's Draft Algorithm Spec
- Review of Several Items:
    - IIP-EXT01 - Extensibility

    - IIP-MA01&MA02 - ALG… DUP
    - IIP-SP02 - Overloading persistent NameID
    - IIP-IDP08 - ForceAuthN
    - Rainer's Strawman:

[Requirement]
Service Provider implementations MUST support the Service Provider Request Initiation Protocol and Profile <<SAML-ReqInit>>

[[Requirement]
Service Provider implementations MUST support a method of IDP-discovery using SAML metadata, either directly or by delegation using the IDP discovery protocol <<IdPDisco>>.

[Guidance]
A well-defined protocol for the SP-first flow provides the capability to either use an IDP derived from the user's context as alternative to IDP discovery.

- Rendered: Rendered Snapshot
    - Source: ADoc Source

Notes

IIP-EXT01 (Extensibility) - section 2.5

"Unless otherwise noted as a required feature" - means: in a reference specification that defines the extension. **AI: Walter will clarify this.**

"Unless" phrase at the beginning doesn't strike one as necessary for interoperability.

That part is trying to counter the optional - there are places in the document (entity attributes) where extension support is required.

Walter will send something to the list on this.

OCLC has an extension defined that causes IdPs to choke - it's not in the assertions, it's in the messages. (example choke:
<samlp:Extensions><oclcns:institutionId xmlns:oclcns="urn:org.oclc.wms" name="institutionId" value="91475"/></samlp:Extensions>
) - identifies a specific institution registry ID (tenant value).

Scott: That's what we're getting at: IdPs shouldn't choke on those.

IIP-MA01 & MA02 ALG … DUP

These are exact duplicates - Rainer intended as one for IdP and one for SP. Scott wonders if those should be moved down under profile requirements for IdP and SP.

Should we delete the dupe? **AI: Walter** will delete the second one in both sections, renumber as appropriate.

IIP-SP02 - Overloading Persistent NameID - section 2.2.1

This targets a problem encountered in Office365 where the semantics of persistent NameID requires more information than the core specification requires.

Is this the right place for this? Mostly targeted at implementations like Office365 that are one-off. They're implementing what their deployment is going to do. Probably fine here. Add a sentence: **AI: Walter** to resurrect original text along the lines of: "Implementations define a custom format if they have additional requirements"

IIP-IDP08 - Force AuthN - section 3.4.1

Eric's proposal

2 Points of follow-up discussion: describing business of modified authN processes in a way that is more obvious; Is this actually a new requirement, or just re-stating the SAML spec? Is it testable?

AI: Walter MUST in second part of the requirement should be capitalized.

AI: Scott to add a period and add a second sentence to normative text: AuthN mechanisms in IdP must have access to the forceAuthN value. Rephrase into something that's more behaviorable/testable. Trying to say what Eric means probably requires multiple paragraphs and examples.

(WILL LET THIS SIT UNTIL ERIC RETURNS IN 2 WEEKS- Scott might propose text in the meantime)

Rainer's Strawman

No follow-up to the proposal on the list from a few weeks back. Scott's recollection is that we decided to drop SP-initiated SSO but require IdPDisco. Scott talked to Rainer about this. Suggested that the requirements to support SP initiated are a subset to support the callback from IdPdisco.

Not clear how much the guidance adds. Walter recommends we strike that.

Walter AI: Add the second requirement (IdPdisco) but not the first, or the guidance, under web browser SSO section.

Next Steps

Next week: "What's the plan for the supplemental algorithm document, how do we link it in?" - will wait for Rainer on that.

Question: There is non-normative text that introduces some sections and sub-sections, but there are some sub-sections that don't contain this type of text. Do we think there has to be introductory text in each section and/or sub-section?

Nate prefers erring on the side of brevity whenever possible. Aim for as much consistency and brevity as possible so people aren't overwhelmed by piles of text wading through the document.

Nick sees this being a case-by-case decision: if non-normative text isn't adding anything, it should be deleted, but it's otherwise of value.

Nick recommendation: Wait until we have the normative text pretty much complete and then go through the non-normative text and whittle down where possible, and add if there is missing.

Agenda - 10/19/2015

- Europe
    -
- Eastern Time Zone
    - Tom Scavo (InCommon/Internet2)
    - Scott Cantor (OSU, Shibboleth Consortium)
- Central Time Zone
    - Walter Hoehn (Memphis)
    - Barry Ribbeck (Rice) - leaving early
- Mountain Time Zone
    - Nick Roy (Internet2)
- Pacific Time Zone
    - Judith Bush (OCLC)
    - Eric Goodman (UCOP)

- Other
    -

Agenda:

- Note Taker: Tom Scavo
- Welcome
- Agenda Bash
- Review of Several Items:
    - IIP-IDP10 - rehash
    - IIP-IDP12 / IIP-SP02 - current location correct or in NameID Section?
    - Should NameID and attribute sections be merged?
    - Dangling requirement at top of the SP section re: NameId
    - IIP-IDP07 - discuss
    - Questions around “ForceAuthn”
- Rainer’s Draft Algorithm Spec
- Rendered: Rendered Snapshot
    - Source: ADoc Source

Notes:

- See below for FIWG TechEx session notes
- Section 3.4.1, IIP-IDP10:
    - ScottC recalls that we decided on the **exact** operator only, but even that simplified requirement doesn’t buy us very much
    - AI: Walter and Eric will alter the text as it stands
- Section 3.4.1, IIP-IDP12 and Section 2.4.1, IIP-SP02:
    - Should we merge these two requirements? For example, in the attributes section?
    - ScottC recommends we leave them as they are now
- Section 2:
    - There’s a dangling requirement re <NameID> at the top of the section
    - AI: Walter will remove this text
- Section 3.4.1, IIP-IDP07:
    - ScottC says there are relevant OASIS errata around this issue
    - One way of phrasing this as an (implementation) requirement: An IdP MUST be configurable to respond to any AuthnRequest
    - Is this primarily a deployment issue?
    - AI: ScottC will review the relevant errata and refactor this requirement.
- Questions around “ForceAuthn”:
    - MikeG has some thoughts that support should be required even if we don't provide explicit deployment advice
    - Eric could more easily write advice than a requirement
    - AI: Eric will propose some text
- Rainer’s Draft Algorithm Spec: Delay until next time

- AI: Eric will compare the document to the list of issues

Agenda - 10/12/2015

- Europe
    - Roland Hedberg
    - Rainer Hörbe
- Eastern Time Zone
    - Tom Scavo (InCommon/Internet2)
- Central Time Zone
    - Walter Hoehn (Memphis)
    - Scott Koranda (SCG and LIGO)
    - Keith Wessel (U Illinois)
    - Barry Ribbeck (Rice)
    - Scott Cantor (OSU, Shibboleth Consortium)
    - Mike Grady (Unicon)
- Mountain Time Zone
    - Nick Roy (Internet2)
    - Nate Klingenstein (Internet2)
- Pacific Time Zone
    - Eric Goodman (University of California)
    - Judith Bush (OCLC)
    - Pamela Dingle (Ping Identity)
- Other
    -

Agenda:

- Note Taker: Nick Roy
- Welcome
- Agenda Bash
- Initial Review of Draft Section 2.5 (Attributes)
    - Rendered: Rendered Snapshot
    - Source: ADoc Source
- **AI: Walter** will pull out the AIs from the last two weeks, organize, and send to the group
- Notes: Review of section 2.5:
    - Replace reference to MACE-dir profile with the X.500/LDAP attribute profile normative document.
    - For the MACE-dir reference, would have to get much more detailed to write testable requirements.
    - Probably no reason to require anything beyond string attribute values
    - If you look at just the SAML 2 bits of the MACE-dir SAML attribute profile, and ignore the targetedID bits, you end up with just the X.500/LDAP attribute profile stuff

    - Not easy to write implementation requirements around, but needs to be in deployment requirements
    - Attribute names should be URIs (commentary section to include text about what we mean by that: “it shouldn’t be so hard to do this that you want to stick a fork in your eye.”) - include requirement for specific name format and testable value to send to test framework.
    - Common problem: integration partner says that they are going to send URI name format for attributes, and then something else shows up
    - **AI: Walter** write something up to reflect this, to replace MACE-dir language in IIP-IDP12
    - IIP-IDP13-17 as a group seem to TomS to be spot on modulo a few changes, might want to possibly modify IIP-IDP13 (reword for clarity) “default attribute release”
    - Scott would like a definition of attribute release policy added if we are going to include IIP-IDP13-17
    - Scott / Eric G would like clarification on default attribute release: “if there is no policy associated with … “
    - Eric G would like combinations of entityID and registration info to be used to calculate policy
    - ScottC says - if you want people to implement booleans (basically Shibboleth attribute release policy language) you have to define all the rest of the requirements around it. Can imagine some pushback on this.
    - Roland: pySAML2 supports 14, 15, 17 but not 16
    - Walter: We need to define “attribute release rules” as opposed to “policy”
    - Walter: proposal: remove IIP-IDP13 and 18 (accepted by the group)
        - (default attribute release, consent)
        - Eric G: my sense is that removing 18 is still being weighed (at least if anyone offers alt text)
    - **Walter AI**: Will drop IIP-IDP13, 18 and renumber everything
    - Scott: If someone wants to write a paragraph of text on consent (in the non-normative section) would encourage them to write that.
- Section 3.5
    - Discussion of corresponding section in SP (3.5): Not allowed to require xsi type or specific hard-coded xsd types; not using friendly name normatively (avoiding common errors)
    - **Scott C AI**: Will write corresponding SP text
    - Orphaned links in this section: would keep metaui requirement - would be a non-normative reference, but worth repeating/emphasizing (IIP-MC01 - add link to metaui)
    - **Walter AI**: Will add link to metaui to IIP-MC01
    - OK to remove idpdisco?
    - ScottC notes: The request initiator spec is more basic (and an easier task for implementors) than the IdP disco spec

- **Rainer AI**: Write requirements for the request initiator spec and send to the list

Agenda (face-to-face at TechEx15, Cleveland, OH October 5)

Attending: Nick Roy, Walter Hoehn, Scott Cantor, Eric Goodman, Gabriel (last name?), Brandon Saunders, Paul Engle, Dean Woodbeck, Harry (last name?), Tom Scavo, Mike Grady, Nathan Dors, Kim Cotton, Scott Koranda, Rainer Hörbe
Scribing: Nick Roy

Intros

Question for the group: structuring of the document - two separate docs - IdP/SP together in one doc or separate?

Walter is in favor of splitting.

Downsides to the split: common references, things getting out of sync, but those aren't likely to happen the way we're authoring it.

There are advantages to one document from a "you can just reference one document" point of view, may be government-related reasons to keep these together.

A lot of monolithic implementations of SAML (no IdP/SP distinction)

Walter's concern is that SP-only implementers might get scared

Scott: Is it possible to fix that via a separate publishing step?

We could put a guide to using this document at the top, helping implementers understand how to use it, where to go for what, etc.

We could do a javascript bit that would hide what you don't need to see if you select options at the top that limit what you need, or do a render-time script to produce two separate documents. Versioning of having two documents would be difficult.

Consensus: Stick with a single document with two sections for now. Can render different views later if need be.

Group Recommendation for Publishing: Anything that is published by InCommon and not Kantara should have "preliminary" stamped on it. Then we want to push it toward Kantara, via REFEDS. For public review, publish on InCommon web site.

Group consensus for publication flow:

Submit to TAC once we are comfortable, with a recommendation for going to REFEDS with good context around it for a time-limited comment period, then make the changes from that feedback period, then recommend it be moved into Kantara for official publication.

Distinction: Implementation profile is for TESTABLE CONDITIONS, and there are things that are just “best practices” that are not testable, that could god into an appendix.

AI for the group: Need to look at all the things that are hard requirements vs. just recommendations/common errors/etc. and figure out what to do with the things that aren’t hard requirements.

Scott would like to remove section 2.1 (Message Flows and Bindings) and add specific sections that account for the behavior that we want. (web SSO, (A)SLO, ECP)

Put all three of the profiles at the end, so, like 2.6 (web SSO); 2.7 ((A)SLO); 2.8 (ECP)

The (A)SLO and ECP sections are just IDP, so could be pulled out of 2.1 and put in an IDP-specific section.

IIP-IDP07 (ECP): SimpleSAMLphp does not support ECP, right now Shibboleth and pySAML are the only known implementations that support it.

Rainer: Not putting this in the profile would kill ECP for a pretty big section of the community.

Putting ECP and (A)SLO separate and moving this to the end would make metadata the first section, which is advantageous.

However, in the SP section, the requirements are so much smaller, it doesn’t make sense to break it apart.

Scott will wait and see what the 2.1 content ends up like (message flows and bindings) before asking to split vs. not.

CONSENSUS: ECP should stay in.

Walter AI: Will create a “Profile Requirements” section and move it to the end, and create subsections for SSO, ECP.

Scott AI: Will write the ECP text in that section, once we finalize the SSO text.

Scott is in favor of, if we keep SLO, making it a “level 2” requirement.

Group consensus: is that we will require SLO, but only to the point of the IdP revoking its session and responding to the SP appropriately. We will require only front-channel implementation. (You MUST do redirect and maybe POST, you MAY do SOAP (backchannel)).

Scott AI: Will write SLO requirements up according to that consensus.

Walter AI: Will convert the items for section 2.1 to prose

Eric AI: Will write up handling of forceAuthn “this is what this is supposed to do, and this is how it might break under different circumstances, might be handled incorrectly” Eric will also call out specific points about isPassive if there is some identifiable degenerate way of implementing this. isPassive works better in that model because you just have to try it and return appropriately.

Walter AI: Will remove IIP-IDP04 and keep IIP-IDP05 (de-duping the “exact” bit) Implications of this is that you CANNOT use technology-specific identifiers on the wire if you are using “exact.”

Mike G AI: Will send suggested nameID text to the list.

Walter AI: Will move IIP-IDP11 into Profiles → SSO section

Rainer AI: Rainer will send his algorithm support draft to the group - he will push it forward though Kantara.

Walter AI: Delete algorithm section, create link to Rainer’s Kantara draft

Group Consensus: SP SLO - don’t require it.

“If you love something, set it free”

Entity attributes: whatever we specify must be testable. In fact, we must define all behavior w/r/t to attribute release that we want to require of the products. With entity attributes, you need to say something like, “must have the ability to bundle sets of attributes for release to entities decorated with user-definable values of entity attributes”

AI: Need a new section to document requirements for entity attributes and handling of them.

Section 2.5 IIP-IDP15/16 are there/cover this, but these are missing something. Need to document the behavior that has to happen to work in our types of federations. This is testable behavior (some of it).

AI: Group should specify those things that are not documented here for an implementation to be able to use support use of attributes the way we want them used in our federations.

Agenda - 9/28/2015

- Europe
  - Roland Hedberg (UmU)
- Eastern Time Zone
  - Tom Scavo (Internet2/InCommon)
  - Scott Cantor (OSU, Shibboleth Consortium)
- Central Time Zone
  - Walter Hoehn (Memphis)
  - Brett Bieber (University of Nebraska-Lincoln)
  - Tommy Doan (Southern Methodist University)
  - Paul Caskey (I2)
  - Mike Grady (Unicon)
  - Barry Ribbeck (Rice)
- Mountain Time Zone
  - Nick Roy (Internet2)
- Pacific Time Zone
  - Judith Bush (OCLC)
  - Eric Goodman (University of California)
- Other
  -

Agenda:

- Note Taker: Judith Bush (OCLC)
- Welcome
- Agenda Bash
- Wrapup of Draft Section 2.2 (continued)
  - Rendered: Rendered Snapshot
  - Source: ADoc Source
- Detailed review of Draft Section 2.3
- Detailed review of Draft Section 2.1

7:05 no other names announced.
Virtual Meeting cancelled next week; F2F at TechX: Roland, Tom S, Scott, Walter, Brett, Eric will be at the FIWG F2F on **Monday, 10/5, 12:10 -- 1:10 pm** in Cleveland

Rendered snapshot generated every 5 minutes

Section 2.2 wrap up

All action items except two assigned to Walter

IIP-CE01 (Common Errors): “It MUST be possible to configure SAML implementations to allow basic interoperability with any peer for which metadata is supplied,....”

Where did we agree this needed to be moved? Metadata capabilities, message flows?

Scott: Message flows section need to be moved down and this can be added. Compare to IDP 01

> (“Assuming SP metadata is available, MUST respond to any valid AuthnRequest. If unable to satisfy a given request, must respond with a SAML error. (this requirement needs work, this is rooted in the general problem of SPs issuing requests to IDPs only to see them fall over or generate errors they don’t get notice of)”)

AI Walter will put it near IDP01 so we can consider them together.

Scott suggests CE01 may be “deployer intervention” focused, no manual step to apply.

Walter: IDP01 is error handling

AI Scott will work on language for replacing the now CE01

Walter has done wordsmithing through 2.2 and has just a few left to edit.(Grammar etc)

AI All: please review 2.2 for the final wording since Walter has done an editing pass.

Brett: ME01 wording, rearrangement looks good

Walter asks: I made up the 307 redirect statement

> **[IIP-ME01]** Implementations MUST support the routine consumption of SAML metadata from a remote location via HTTP/1.1[RFC2616] on a scheduled/recurring basis, with the content of the metadata automatically applied upon successful validation. HTTP/1.1 redirects (status codes 302 and 307) MUST be honored.

Brett thinks this makes good sense.

Scott wants a permanent redirect honored. Walter: Is this the correct way to specify this? Scott: This is how this must be done.

AI Walter will check on the permanent redirect code to verify according to HTTP spec

Tom says HTTP 301 is the permanent redirect

When do we rationalize IDs? As we go

Question re numbering due to the IDP vs SP numbering.

AI Walter Adding the should SP

Section 2.3 Name identifiers

[IIP-NI01]

> Implementations MUST support the following SAML V2.0 name identifier formats, in accordance with the normative obligations associated with them by [SAML2Core] sect. 8.3):

- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Scott raises the following:

- Req name id selection format behavior based on specific content in the metadata
- are these two sufficient in light of how the cloud works - cf commercial SPs, name IDs vs attributes

Eric seconds the consideration that these two may not be sufficient.
Scott: is Shibboleth the outlier?
Walter: these are the only formats that will work with interoperable by default.
Scott: really, just transient as persistent also makes assumptions
Walter: says with a reasonable configuration you can have a reasonable interaction with persistent
Scott asserts that email address is not necessarily an address, but just looks like an address.
No agreement on what that meant. The two above were EXPLICITLY defined. But in practice we don't know what people do with persistent. Let's add requirements around triggering with metadata because this is Non Normative in the metadata spec.
Walter asks: for persistent, is there text in the spec about mutual understanding, or is it opaque to the provider. Meant to be opaque to the SP, but isn't necessarily so.
Office 365 wants persistent but not …
Mike Grady: qualified by SP, pairwise?
Scott: yeeeesssss, but the IDP is allowed to say the world is the other end of that pair.
Scott says if you get something that looks like an email, go ahead and log it because that's what they've chosen. It IS meant to be not public, limited disclosure, association with identity not easily associated.
Eric is INTENTIONALLY not saying anything on this topic.
Scott: As an SP you are not allowed to dictate to the IDP what goes in the values as long as it follows the rules. The GUID Microsoft asks for is NOT CORRECT BEHAVIOR. Make your own definition. << Goes in the SP section
Walter says we should add unspecified to the spec
Eric agrees that "Define your own format" should be a recommendation to the SP.
AI Scott will write some text around the IDP side (select formats based on metadata)
AI Walter will propose re the SP needs to define new instead of demanding misuse of the existing specified name formats. Will verify details. Also will include the unspecified format in this SP section.

Mike Grady: Tom Scavo (or maybe Nate K?) ran into this with simpleSAML as well…. it always requests a nameID. (Scott) There isn't a requirement that one sent in the standard. Clearly if the SP asks one the IDP should send or fail. You can't configure the simpleSAML SP to NOT send a request. You need to change the code...
Scott agrees that seems like a common error.

Mike was surprised by the number of IDPs NOT configured to send transient in Name ID.
It's another surface of issues when looking for minimal attributes. This DOES cause issues in interop.
AI Mike will come up with a description for this.

2.1 Message Flows and Bindings
What is the distinction between IDP04 & 05?

> **[IIP-IDP04]** MUST support all SAML-defined `<RequestedAuthnContext>` operators (exact, minimum, maximum, better)
>
> **[IIP-IDP05]** MUST support the "exact" `<RequestedAuthnContext>` operator (returning an error or selecting from among multiple login methods, as appropriate)

Scott: alternatives?
Scott: we should have a section for each profile. One on browser SSO, one for ECP (if it were a must), and then we need to decide about Logout….
Walter: start with requirements, Scott: but w/o the profiles these are confusing.
Walter Does IDP06 & 07 need to be there?

> **[IIP-IDP06]** MUST support the SAML V2.0 SingleLogout profile (in SAML2Core) and the SAML V2.0 Asynchronous Single Logout Protocol Extension [SAML2ASLO]
>
> **[IIP-IDP07]** MUST support the SAML V2.0 Enhanced Client or Proxy Profile Version 2.0 [SAML2ECP] with applicable requirements pertaining from the Browser profile requirements noted in the Basic requirements above

Scott: quite onerous… 04, 03 seems over much as just one seems sufficient...Guesses Riener would push back
Walter: why is post in MSG01?

> **[IIP-MSG01]** MUST support the HTTP-Redirect and HTTP-POST bindings for requests

Scott: not onerous, some things won't work right (office links, links in office documents)
Tom was not the original author.
Scott says MFA may be studying some of these use cases… Scott leans towards saying support all four.
Tom says if we are going to err, err in overspecifying. (Choose IIP-IDP04)
Consensus is to choose IIP-IDP04 but weak - -should we post out questions?
Scott does SimpleSAML, FORGERock (esp) support?
Eric thought 4 &5 come at different times and 5 calls out a special meaning of exact. Thinks that people claim "sure i support" but behave in unexpected manner.
Walter Common errors?
Scott: Timestamp usage is an example of presumably clear spec but many different implementations
AI Eric will take force authN

[IIP-IDP07] MUST support the SAML V2.0 Enhanced Client or Proxy Profile Version 2.0 [SAML2ECP] with applicable requirements pertaining from the Browser profile requirements noted in the Basic requirements above

Scott: title is incorrect because Logout
AI Nick will clean up title & intro to include Logout ...
Walter & Scott discuss ECP while recording flails.
Scott's personal feeling is he would like to see ECP required, believes needed for research community.

Agenda - 9/21/2015

- Europe
    - Rainer Hörbe
- Eastern Time Zone
    - Scott Cantor (OSU, Shibboleth Consortium)
    - Tom Scavo (Internet2/InCommon)
- Central Time Zone
    - Paul Engle (Rice)
    - Paul Caskey (I2)
    - Scott Koranda (LIGO and SCG)
    - Tommy Doan (Southern Methodist University)
    - Brett Bieber (Nebraska)
- Mountain Time Zone
    - Nick Roy (Internet2)
    - Ames Fowler (Aegis Identity)
- Pacific Time Zone (it's early on the West Coast!)
    - Walter Hoehn (The University of Memphis) (did Memphis move?)
    - Eric Goodman (University of California)
    - Jon Wall (Microsoft)
    - Judith Bush (OCLC)
- Other Time Zones

Agenda:

- Note Taker: Nick Roy
- Welcome
- Agenda Bash
- Detailed review of Draft Section 2.2 (continued)
    - Rendered: Rendered Snapshot
    - Source: ADoc Source

Notes from 9/21/2015:
Goal: Identify any remaining work, create action items for each remaining work item
Additional: Discuss Rainer's additional work, where it goes in the document

Fair amount of discussion on Rainer's proposal on the list
Inclusion in section 2.4 or 2.2?
Rainer: Merge request into 2.2 after 2.2.4
Scott: Agree with that, would move the algorithm requirement to a separate document, add the schema to the list of schemas at the top
Walter: Received the merge request, and a cancellation
AI: Walter will merge per request
Rainer: Accepted Eric's suggestions on language
Walter: Thanks to Walter to for doing this
Scott: IIP-IDP10 is a stray requirement that should come out, be replaced by Rainer's content
AI: Walter will pull out IIP-IDP10
Scott: Should pull the 2.2.4 stuff up to Metadata Exchange
AI: Walter will relocate the MDQ stuff into the Metadata Exchange section
AI: Walter will make each section its own adoc - all the metadata sections will become their own document. Goal: Move IdP-specific metadata exchange requirements up into main metadata section. Benefit: Can get rid of "???" section.
Scott: Making MDQ: IIP-IDP08/09 (MDQ) are a MUST for IdP, should also be a SHOULD for SP. Would prefer to make a level 1 and level 2 conformance requirement, and make it a MUST for SPs at level 2.
Walter: Not against having levels of conformance, but it should be more broadly applied, not just for MDQ
Scott: It would be more broad
Walter: Let's make it an SP SHOULD for now, and then later we can add the conformance levels later.
AI: Walter will make IIP-IDP08/09 (MDQ) a SHOULD for SPs
Scott: Parallel burden for SPs to deal with discovery (difficult with MDQ) and MDQ. Compromise is to make it a MUST for IdPs and SHOULD for SPs.

Walter: Two subsections feel pretty good about. Would like to agree we are basically done with: 2.2.1 and 2.2.5. Both have gotten quite a bit of working through on the list. Please take a look at these briefly.
Scott: In 2.2.5 since these are "common errors" it's awkward to have them be MUSTs
Walter: That's for testability
Rainer: Metadata capabilities (2.2.1) are very minimal - MDUI for discovery; Algorithm support is a separate topic; Registration information - these three things come to mind.
Scott: It's hard to include feature things without encroaching on UI design. Most of all, it's not testable.

Rainer: In a deployment profile you could test that it's loadable, but would be hard to test the UI implications of this.
Walter: Is referencing other standards as requirements awkward?
Scott: AI: Will add some introductory text on this part (intro to requiring support of separate standards in 2.2.1)
Eric: MD-IOP in IIP-CE01 is difficult for, say, Okta because it is counter to their model.
Scott: Right, but that's an outlier
Scott: This is about supporting multilateral federation, if it's an explicit requirement, it should also be somewhere else besides "Common Errors"
Walter: Yes, this seems fundamentally different from other requirements - probably needs to be pulled out and called out for support elsewhere.
Walter AI: Will reorganize this into a different subsection
Scott: Should be in a section where we will move the message flows and bindings. Subordinate to how you generally have to process the requests and support the profiles.
Scott: Should pull out IIP-IDP01 - thought we had pulled this out, but have not. It's not testable, it should be pulled.
--->AI: Discuss pulling IIP-IDP01 on list? Or just do?
Walter: IIP-M07 has been iterated on the list - are we OK with that?
Tom: Wording optimization that could occur- **AI: Tom will propose on the list.**
Walter: IIP-M06 is much the same - gotten a lot of traffic, probably OK at this point, like to make sure. No discussion (looks good).
Walter: **Brett AI** follow-up on splitting apart IIP-M05 - Brett was going to add IIP-M05 on redirects. IIP-M04 is the first part of the split, looks good.
Tom: Question whether IIP-M05 needs to be a MUST: For example, HTTP conditional GET - if a client is just refreshing once a day, that's fine without supporting conditional GET.
Walter: I'm OK with M05 being a SHOULD
Scott: Really don't think that SHOULDs accomplish anything, just pull them
Walter: What is it that we get from including M05 at all?
Tom: There's value on the server end: optimize your server environment knowing these two items are supported. Server/network folks where Tom is don't worry about serving large metadata files. If these don't concern anyone on the server side, why are we putting requirements for them on the client side?
Walter: Anyone opposed to just deleting IIP-M05? (No discussion - OK to delete)
Walter AI: Will delete IIP-M05
Scott: Putting redirect handling in IIP-M04 is fine. Brett keeps his AI.
Brett AI: Put his redirect text into IIP-M04 instead
Walter: At this point we are left with 2.2.3 - the text as it stands now is a raw pull from the draft on the wiki. No work on the list so far.
Tom: I don't think IIP-M09 is a strict requirement. It's not absolutely necessary for key rollover to support multiple keys in MD.
Scott: But it is required if you ever want to move off of RSA (change algorithms) then you must support multiple keys in MD.
Tom: OK, I see what you're saying, I withdraw my comment.

Scott: Most likely choice to move to will be EC keys, but don't know when that will be.
Walter: Feel like the content here is what we want, just need some wordsmithing
Scott AI: Will wordsmith all content in 2.2.3 - but content looks good
Walter: Initially, had discussed trying to make each requirement standalone - if we are going to reference other material, should be more explicit. Mostly cleaned that stuff out.
Scott: IIP-IDP09 should be a duplicate of IIP-M06 - techincal requirements are coming from M06. There is also an extra sentence in M08 that needs to come out.
AI Scott: will do a pull request on all of these and fix up, **after Walter moves things around.**
Walter: We now have AIs for all of section 2.2.
Scott: Would like to request that people who have not implemented this model, please review. Also need to add explanatory text as context - but need review from people who don't currently support this to help us know how to provide this context.
Walter AI: Will script rendering so the render stays up-to-date every few minutes.
Walter/Nick AI: After 2.2 complete, ask for feedback on list from implementers that don't currently support this model - possibly seek wider feedback.

Planning to attend F2F at TechX: Nick Roy, Walter, Scott K, Rainer, Scott C (if no overlap), Paul Engle (don't know schedule yet though), Eric G, Tom S

Walter: Section 3 - currently listed as Name Identifiers, no text there at all. Assumption: Pull in very small number of requirements that facilitate what's in saml2int. Walter can get started on that. Any opinions on content?
Rainer: What proposed with eGov 2.0: requirements that support saml2int
Rainer AI: Will forward that content to the list
Walter: Appreciate that, thanks
Scott: It MAY be worth calling out some requirements around driving selection, process by which right type of nameID is selected. There is an inband way to do it that are part of SAML 2 itself, but there are other ways that are driven by metadata that may be a good way to call out.
Walter: That's certainly an area where there are things in the wild causing problems. Important that we deal with it in a real way that is helpful.

Agenda - 9/14/2015

- Europe
    - Rainer Hörbe
- Eastern Time Zone
    - Tom Scavo (InCommon/Internet2)
    - Scott Cantor (OSU, Shibboleth Consortium)
    - Steve Carmody (Brown)
- Central Time Zone
    - Walter Hoehn (University of Memphis)
    - Barry Ribbeck (Rice)
    - Scott Koranda (LIGO and SCG)

    - Brett Bieber (University of Nebraska-Lincoln)
    - Tommy Doan (Southern Methodist University)
    - Paul Caskey (I2)
    - Mike Grady (Unicon)
    - Kim Cotton (University of Missouri)
- Mountain Time Zone
    - Nick Roy (Internet2)
    - Ames Fowler (Aegis Identity)
    - Nate Klingenstein (Internet2)
- Pacific Time Zone (it's early on the West Coast!)
    - Eric Goodman (University of California)
    - Judith Bush (OCLC) (must leave at 7:30 am PDT for another meeting)
    - Pam Dingle (Ping Identity)
- Other Time Zones

NOTE: announce name before making comments
NOTE: when making an important point, be sure to check the scribing document and make sure that it has been documented accurately

Agenda:

- Note Taker: Eric Goodman
- Welcome
- Call for Scribes:
    - https://spaces.internet2.edu/display/FIWG/Meeting+Scribes
- Agenda Bash
- Detailed review of Draft Section 2.2
    - Rendered: Rendered Snapshot
    - Source: ADoc Source

Notes from 9/14/2015:
Scribing Volunteers:
- Nick Roy (9/21)
- Judith Bush (9/28)

Rainer: How complete is section 2.2? Specifically Entity Attributes and (specifying) Encryption Algorithms.
- We should verify the list of requirements against the "issues" list (presumably: https://spaces.internet2.edu/display/FIWG/Interop+Issues+List)
- Scott: Not an exhaustive list of all extensions must work or be parseable, I.e., not a duplication of the spec.
- Encryption specific discussion:

- Eric: Should clarify supporting specific algorithms (in messages) vs. identifying support in metadata
    - On Algorithm side, was explicitly(ish) excluded in early TAC calls
    - Walter: Agrees that extensions are not listed in 2.1, where they might go
    - Scott C: Perhaps language that extensions must be able to be parsed (not "crash" on them), and then calling out specific extensions that we are recommending/requiring.
    - Rainer: EU would really like to have "mandatory" support in metadata for expressing encryption support.
    - General question: Should encryption extension supports be required?
        - Scott C/Rainer: Leaning towards support on IdP being required, but not nec. required in the SP
        - Scott C: But not as useful if not required on both sides
    - **Action Item: Rainer to put together straw man "encryption extension" support section - send to list**
    - **Action Item: Walter will pull out section 2.1 extension text and reformat, let Scott C know so he can update it (next AI)**
    - **Action Item: Scott C to put together separate strawman section on extension for metadata - send to list**
- What about Entity Attributes?
    - Scott C's point: parsing and handling entity attributes a software feature, not part of the SAML spec, so wants to clarify that having requirements on how entity categories are used to manage SP support is extending beyond SAML specs.
    - Some sense that entity attribute parsing may belong in its own section, since it's beyond the general requirement called out before about "not choking on arbitrary extensions in metadata". But could stay 2.5. So long as it's clear that this is a special case (and not the totality of metadata extension support).
    - The only concrete use case we have today for entity attributes is around attribute release policies.
- Scott C notes: The current text ([IIP-IDP12, 13, 15, 16] in 2.5 Requested Attributes and "attribute release policies" are written in "Shibboleth"-centric language

Began walking through the sections in 2.2..

- No comments on M01/M02
- M04: Should version "http" (1.1, 2, etc.) to be clear what is expected
    - **Action Item: Walter will clarify http version**
    - Pam: has a MUST and a SHOULD in the same requirement. Should those be two different conformance statements (for testing purposes)?
        - Pam: Having more atomic requirements is nice for vendors from the standpoint of being able to be clearer about what they support and can provide a "PR"-type value in terms of showing what is supported.
    - Can this be a MUST?

        - Tom: Thinks that conditional GET is more important than compression, so would like to see these separated, especially if this becomes a MUST
        - Walter: Is there a burden/cost to implementers to support conditional get (that would make MUST a problem)?
            - For the most part, seems like no, but calling it out is valuable just to provide clarity to implementers
        - Compression seems like it should be a "MUST" today, but you need to call out the specific features/specifications (e.g. inflate/deflate)
    - **Action Item: >>>WHO???<<< Move conditional GET to MUST, move compression to a separate bullet that is a SHOULD**
- Brett: Do we need to provide recommendations on how to handle redirects encountered when accessing metadata via URL?
    - **Action Item: Brett will propose straw-man language**
- Tom: Thinks M06 needs language to specify where the attribute should occur. Language on the terms "verification/verify" and "validity/validate".
    - Walter: Typically certs are "verified" not "validated", whereas XML is "validated"
    - Verification is where you use a specific kind of technical procedure, validation is when you use a higher-level process to check the "okayness" of a thing
        - **Action Item: Walter to send text of a new RFC distinguishing the two to the list**
    - Scott C: "Must limit metadata acceptance" based on validUntil
    - **Action Item: Tom to send strawman attempting to use "acceptance" not "verify" or "validate"**

Meta-conversation (not metadata): Should "SHOULDs" be included in the conformance statements?

- No consensus (both opinions, "yes" and "no" expressed in roughly equal volume)

Agenda - 8/31/2015

- Europe
    - Roland Hedberg (SWAMID)
    - Rainer Hörbe (Kantara, ..)
    - Nicole Harris (GEANT)
- Eastern Time Zone
    - Tom Scavo (Internet2/InCommon)
    - Scott Cantor (OSU, Shibboleth Consortium)
    - Brandon Saunders (IDM Integration)
    - Steve Carmody (Brown Univ)
- Central Time Zone
    - Tommy Doan (Southern Methodist University)
    - Barry Ribbeck (Rice)
    - Walter Hoehn (University of Memphis)

    - Brett Bieber (U of Nebraska-Lincoln)
    - Scott Koranda (LIGO and SCG)
    - Kim Cotton (University of Missouri)
    - Mike Grady (Unicon)
- Mountain Time Zone
    - Nick Roy (Internet2 Trust & Identity)
    - Nate Klingenstein (Internet2)
    - Ames Fowler (Aegis Identity)
- Pacific Time Zone (it's early on the West Coast!)
    - Judith Bush (OCLC)
    - Eric Goodman (University of California)
    - Russell Beall (University of Southern California)
- Other Time Zones

Agenda:

- Note Taker: Barry
- Welcome
- Agenda Bash
- Summary from last week's call
- Review "Interoperability Issues List" (led by Eric G.)
    - https://spaces.internet2.edu/display/FIWG/Interop+Issues+List
- Review strawman format for implementation spec
    - Rendered: http://walterhoehn.com/dl/SAML-Impl-Profile/rendered/SAML-ImplProf.html
    - Source: http://walterhoehn.com/dl/SAML-Impl-Profile/adoc
    - Questions related to the overall structure
        - Overall look
        - Shared material vs. IdP or SP-specific items
        - Requirement Identifiers
        - Appropriate Sectional Breakdown?
        - Prose?
    - Review requirements from section 2.2 "Metadata and Trust Management" in detail
    - Discuss Rainer's comments re: Kantara eGov overlap (9:45)

Notes from 8/31/15
AI: Volunteers for revolving note taking to be looked at by Walter
Eric - Begin discussing Interop work see email for bullet points spread sheet. Reminder that 2nd column is an interpretation of Eric not part of the spec.

Walter - begin by discussing format and request for issues raised by others. Identify responsibility by person bringing question or issue. Separation also could be defined around community practices as well. Items that were agreed to be tabled should not be lost. There should be a column to map to link each line item to a spec. Every requirement should have a separate identifier.
Things discussed in email or other discussions should be captured in the wiki.
AI: Walter will go through previous notes and email threads that may need to be back populated.
AI: All: enter any tabled items you have into this wiki, note yourself as the responsible party as a placeholder
Strawman Implementation Profile discussion:
Need separate identifiers for each requirement
Wanted separate requirements for IDP and SP but could share references.
Example: In the IDP doc, the metadata section for encryption, etc all are separated out. The structure provided is granular but has a potential drawback of having to make many changes if order changes.
General agreement on the identifier format. Clarification if you look at an identifer, and it contains IDP or SP then the identifier is specific to IDP or SP, so not general requirements.
Barry's simple examples (annotation on the requirements) that show implementers the cases, reasons, real-world examples for doing things certain ways.
Roland: This is very useful, if you write something down as a requirement with room for interpretation, it will get misinterpreted. **Most important thing: capture these as testables, agree on the test requirements.**
Is this group resourced to derive test requirements?
Comments for section 2.2?
From language pulled from the draft profile. All requirements should be changed to correct grammar. Some of the references do not link up correctly, IIP-M03 - found the language confusing.
Some of the requirements may not be able to be met by some providers regardless of the reason. If the requirement is in eGov should it be assumed that it is fair to add and assume that it will be implemented? Scott's example - Will Box be able to meet these minimum requirements?
The document should stand alone without relying on.
Homework items - define basic INTEROP, provide feedback on the list for section 2.2 (Metadata and Trust Management: (thanks Nick)
http://walterhoehn.com/dl/SAML-Impl-Profile/rendered/SAML-ImplProf.html)
AI: Walter will synthesize comments from the discussion on the list, update this section
RAINER: discussion of method for most impact using previous work Kantara and eGov. See emailed spreadsheet regarding the overlap of requirements. Goals stated are alignment with other work that could be easily adopted, eliminate forks,
Nick - the question needs to be vetted with TAC as a strategy for moving forward? Nick had some implementation questions.

AI: Nick and Keith H will talk to TAC, probably ask Walter to call in for Thursday's TAC call

In the spreadsheet the requirement column comes from eGov.
Scott - objected to logout in eGov (very difficult to do - SOAP requirements) and questions if it should be in a base spec. Should some of these requirements could be softened or removed? Focus on the base layer could scope our work. Additional layers could bring in broader requirements.

ACTION ITEMS:
Present Rainer's proposal items to the TAC(Nick/Walter)
Everyone should review proposal 2.2 (All)
Gitlab work to proceed (Scott K/Walter)
Action item to invite larger group - after discussion with TAC(Nick/Walter
Review previous minutes for content to go in Eric's requirements matrix (Walter)

Agenda - 8/24/2015

- Europe
    -
- Eastern Time Zone
    - Scott Cantor (OSU, Shibboleth Consortium)
    - Tom Scavo (InCommon/Internet2)
    - Brandon Saunders (IDM Integration)
    - Steve Carmody (Brown)
- Central Time Zone
    - Walter Hoehn (University of Memphis)
    - Barry Ribbeck (Rice)
    - Scott Koranda (LIGO and SCG)
    - Brett Bieber (U of Nebraska-Lincoln)
    - Tommy Doan (Southern Methodist University)
    - David Langenberg (University of Chicago)
    - Kim Cotton (University of Missouri)
- Mountain Time Zone
    - Nate Klingenstein (Internet2)
- Pacific Time Zone (it's early on the West Coast!)
    - Judith Bush (OCLC)
    - Eric Goodman (University of California)
    - Russell Beall (University of Southern California)
    - Andrew Hughes (Independent Consultant)
- Other Time Zones
    -

Agenda:

- Welcome
- Agenda Bash
- Summary from last week's call
- Technology used for editing/publishing the document
    - Rainer's proposal
        - asciidoc/github
        - http://htmlpreview.github.io/?https://github.com/rhoerbe/SAMLprofiles/blob/master/rendered/WebSSOScaleFedProfile.html
- Compiling list of common interoperability problems
    - "Kicking things off" thread
- Begin detailed discussion of the "DRAFT SAML Implementation Profile" https://spaces.internet2.edu/display/InCFederation/SAML+Implementation+Profile
    - Is the overall structure what we want?
    - Dig into the IdP Requirements Section

Notes from 8/24/2015

Summary from last time:

- Discussed three feed documents
- OASIS doc probably isn't relevant for our work here
- How are we are going to handle crypto requirements?
- Consensus: The Draft SAML Implementation Profile is probably closest to what we need at this time but portions of the Kantara doc could be used as well
- Audience: implementers of SAML products
- Consider IdP and SP requirements separately if possible

Technology used for editing/publishing the document:

- Piggyback on Rainer's method involving asciidoc/github
- Brett appreciates the proposed method (but is not familiar with the technology)
- Barry likes the page layout and the fact that it can be modified as desired
- Walter suggests we stick with the default templates for simplicity
- Is github accessible to everyone?
- Is federated login to github possible? gitlab?
- LIGO has a federated gitlab instance. ScottK is willing to stand up another one.
- **AI:** Walter will followup with those who have contributed to the discussion

"Kicking things off" thread:

- Good thread
- Should we capture the essence of that thread in the wiki?
- Is there a volunteer?
    - **AI:** Eric will edit a first draft

    - **AI:** Judith will contribute her notes

Reviewing the the “DRAFT SAML Implementation Profile”:

- This document came together quickly, so document format was not well thought out
- ScottC is not a big fan of the matrix format (i.e., heavy use of tables) but tables can enhance the overall presentation of requirements
- Do others feel comfortable with the current format of the document?
- The content re metadata is (intentionally) presented early on in the document
- Should SP and IdP requirements need to be separated out? The comments seem to indicate the answer is yes, so let’s separate IdP and SP requirements into their own sections
- What about the material on key rollover? Can that be separated into IdP and SP portions?
- Walter and Scott wonder if we might end up with two documents: one for IdP implementers and one for SP implementers
- On the down side, two documents make it more difficult to do cross-references
- Barry suggests the audience be clearly spelled out
- Judith suggests we may be able to have multiple “views” of the document content: one comprehensive document and/or focused documents as needed
- Task: Convert the wiki document into the new format
- Steve suggest we first produce a skeleton document so that multiple people can start working on the details
- **AI:** Walter will take a first crack at porting the document to github
- Once the content has been migrated to the new format, individuals can start working on the various sections of the doc

---

Agenda/Notes Archive of Previous Calls

8/17/2015 Call

Attending:

- Europe
    - Rainer Hörbe
    - Roland Hedberg
- Eastern Time Zone
    - Scott Cantor (The Ohio State University / Shibboleth Consortium)
    - Tom Scavo (InCommon/Internet2)
- Central Time Zone
    - Barry Ribbeck (Rice)

    - Walter Hoehn (University of Memphis)
    - Brett Bieber (U. of Nebraska-Lincoln)
    - Mike Grady (Unicon)
    - Kim Cotton (University of Missouri)
    - Tommy Doan (Southern Methodist University)
- Mountain Time Zone
    - Nick Roy (Internet2 Trust & Identity)
    - Nate Klingenstein
    - Ames Fowler (Aegis Identity)
- Pacific Time Zone
    - Andrew Hughes (Independent Consultant)
    - Judith Bush (OCLC)
    - Russell Beall (University of Southern California)
    - Dedra Chamberlin (Cirrus Identity)
    - Eric Goodman (University of California)
- Other Time Zones

Agenda and Notes 8/17/2015

- Welcome
- Agenda Bash
- Reflections on feed documents for an implementation profile:
    - "Conformance Requirements for the OASIS Security Assertion Markup Language V2.0"
        - http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf
    - "DRAFT SAML Implementation Profile"
        - https://spaces.internet2.edu/display/InCFederation/SAML+Implementation+Profile
    - “Kantara eGovernment Implementation Profile”
        - http://kantarainitiative.org/confluence/download/attachments/38929505/kantara-report-egov-saml2-profile-2.0.pdf
    - Strengths/Weaknesses of these documents
    - In what ways do these documents help to address common interoperability problems?
    - Are there other problems that we have identified that could/should be dealt with in an implementation profile?

- The Scoping Question…
    - Defining the audience for an implementation profile
    - What are the consequences of a decision with regard to the scope?
        - Contents (Focus on metadata vs. more complete profile)
        - Applicability (SAML Products vs. One off implementers)

        - Lifecycle (One-time vs updateable vs. composable)
        - Uptake (do the answers to these questions dictate our success)

- First Steps
    - Is the “DRAFT SAML Impl Prof” a good starting place? The Kantara profile?
        - edit or replace
    - Technology used (email, wiki, MS Word, Google Doc, git/markdown, other)
    - Volunteers to draft a list of items that should be addressed in the profile
    - Volunteers to draft suggested changes (if we are starting from a pre-existing document)

Discussion:

- Rainer has made an editing structure for the saml2int doc, just a technical structure for how to do the editing, making requirements referencable, etc.
- Reflections on feed documents for an implementation profile:
    - "Conformance Requirements for the OASIS Security Assertion Markup Language V2.0"
        - http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf
        - Originally published in Mar 2005 - long history makes it easy to judge its success or lack thereof. A revision of the OASIS SAML V2.0 Conformance document (with errata) was published in Dec 2009
        - It is the product of vendor compromise, as well as OASIS requiring a conformance statement even when it wasn’t really possible to construct one in the absence of deployment experience. Large amount of information pulled in from Liberty Alliance community vs. very tightly scoped vendor desires. Vendors had a more minimalist view of requirements. The metadata spec is entirely derived from the Liberty Alliance contribution. The compromise was to make metadata purely optional.
        - Rest of the document was compromise between Liberty community wanting advanced profiles like nameID management that no one used. Figuring out what of that stuff was going to be required vs. optional took much of the rest of the time.
        - While it was the basis of getting the early brand marks that Liberty was granting for SAML conformance, people were implementing to the test and ignoring what was needed in a real world scenario. Conforming to the spec didn’t necessarily guarantee interoperability.
        - The grid has things numbers of us haven’t heard of.
        - The difficulty is lack of support for the details of things inside the SAML messages - you can be conformant but not support the necessary details

- The crypto requirements in the spec are not just outdated, they're actively harmful at this point. Standards don't move fast enough to keep up with crypto guidance. The market doesn't want a product to have to change to meet conformance every 3 months when crypto best practices change. There needs to be a shared crypto standards body as part of IETF or some other body that takes up that charge.
- Does a possible solution to the security issue involve making the security requirements composable and updateable on some regular schedule? Yes. However if you expect a lot of commercial vendors to support this it's unlikely to be successful. Recommend that we park this as an agenda item to avoid rat-holing. Agreement.
- Feature matrix: A lot of stuff labeled 'MUST' that are not necessary for most of our use cases, other stuff that is important that people don't follow - section on encryption.
- Do we lose people with the size of the grid? Likely
- Do we lose people when they have to go reference-chasing on things like security? Likely - also W3C is a bit different from other standards bodies and that makes things more confusing
- Security: [SURFnet will NOT connect to SPs that do not pass a certain level of TLS security: "need a minimal rating of B on SSLLabs (https://www.ssllabs.com/ssltest/analyze.html)"] Not something we shouldn't address, but something we should address at a later date.
- ScottC: "Addressing it today is easy, addressing it in 6 months is the problem."
- This is a document we would not want to specifically reference - true? General agreement.
- ScottC: Something to do nameID management is a huge problem across federations, it's just that no one has done it/implemented it. Most of us have a lot of applications that use name-based identifiers and management of those across federated apps is still a huge problem.
- Something that applies to all three documents: For our purposes, even for the profiles that we want to support, is it necessary to require all of these bindings for those profiles, as opposed to saying, "here are the recommended bindings, that's what you MUST do, everything else is MAY"?
- Should we nail down the specific set of bindings in our profile? Yes, but artifact is a tougher quandary b/c OpenID is largely artifact-based. Suggests that getting rid of the back-channel is not going to be something that happens any time soon. The off-the-cuff goal might be to get rid of artifact as a required binding. The more we can pull things out that we don't need, the more important it makes the things we do care about seem important to implementers.

        - Being too geared toward higher-ed might hurt the effort because it's a sector-specific thing.
        - Proposed scope: set of use cases that are common to higher ed deployments, but not unique to those deployments.
        -
    - "DRAFT SAML Implementation Profile"
        - https://spaces.internet2.edu/display/InCFederation/SAML+Implementation+Profile
        - This document grew out of a need expressed by Steve Carmody, chair of InCommon TAC, in June 2015
        - Apparently two vendors came forward at the same time: Ellucian/Banner and Microsoft Azure AD
        - Steve wanted a list of requirements to frame the discussion with these two vendors
    - "Kantara eGovernment Implementation Profile"
        - http://kantarainitiative.org/confluence/download/attachments/38929505/kantara-report-egov-saml2-profile-2.0.pdf
        - Rainer would recommend not using sector-specific language in our profile (egov, for example) because it makes the document, which is widely applicable, seem sector-specific.
        - Nick: This looks like a very robust place to potentially start.
        - Worth heavily cribbing from
        - Format is closer to what we want than what we have in the draft SAML implementation profile that's currently on the wiki
        - There is quite a bit in there about artifact binding requirements
    - Strengths/Weaknesses of these documents
        - Should we take what we are working on and compare it to the saml2int doc, etc. to make sure they are compatible?
        - NameIDs, on a practical level, there are a significant number of incompatibilities, it would be nice if we provide guidance that tries to make nameID treatment clear for implementers/deployers.
        - Could remove things that aren't needed - PKI, etc.

- The Scoping Question…
    - Defining the audience for an implementation profile
        - Are we trying to say people should do metadata, or should we try to do more? Also question of SAML vendors vs. application-specific SAML implementations. Roland and OCLC (Judith Bush) consider themselves implementers, are on the call. Roland went through the documents and tried to implement everything, and did. At the same time, wondered how much this is ever going to be used (nameID management stuff). OCLC: Andy Dale was original architect, some things that he said we had to implement, that haven't yet. Some things like key rotation, that know they

have to support, that haven't done. Judith thinks this is extraordinarily useful for both those that are writing their own SAML implementation, and those that are integrating using existing software. So, answer is, the audience should be "both" - SAML implementers and app-specific SAML support. Nate: Would recommend taking the requirements from deployers, have the end product aimed at implementers so that the deployers can implement that.
        - There is a fairly natural split between IdP and SP and we need to start talking about that. It would be reasonable to scope down the SP requirements. There are a lot of SP things that can be done by an application. There are things that are done by an IdP that are really more oriented toward a SAML implementation. We can be more aggressive with requiring things of IdP implementation.

    - What are the consequences of a decision with regard to the scope?
        - Contents (Focus on metadata vs. more complete profile)
        - Applicability (SAML Products vs. One off implementers)
        - Lifecycle (One-time vs updateable vs. composable)
        - Uptake (do the answers to these questions dictate our success)
            - When it comes to what vendors do and how they support this profile, there is room to tell stories about vendors that may not have implemented enough to support this federation model, realized that they needed to, and went back and did that and had greater success.
            - Use cases: we all have these things in our head, but it's not something that we've spelled out.
            - California Community Colleges have joined InCommon and have apps that they want to share. There may be some use cases there. Others in this group have stories about vendors who saw success from integrating with InCommon. **AI: Dedra, Walter and Nick will sidebar about this.**
- Guiding principles:
    - Don't include things we don't need in the document
    - Specification of the profile should be usable for implementation of a test harness
    - Requirements should be worded context-free (no requirement interdependency)
    - Repository of test cases should be able to easily reference this
- **AI: Walter** will synthesize the discussion from today and communicate to the list. Will move the third item of the agenda (first steps) to the list.
- Final note on enc from ScottC: A lot of the stuff around XML encryption will need revisiting in light of the current state of XMLenc (broken) and a lot of the existing interop difficulty is around support for XML encryption.
- Mike Grady: Supporting discovery on the SP side - necessary for our use cases. Right now, lack of support for discovery is driving people toward use of proxies.

- First Steps item from agenda to be addressed via the mailing list this week in prep for next call

---

8/10/2015 Call

Attending:

- Europe
  - Rainer Hörbe (AT government)
  - Nicole Harris (GÉANT)
  - Pam Dingle (Ping)
- Eastern Time Zone
  - Scott Cantor (OSU / Shibboleth Consortium / InCommon TAC)
  - Gregory Katz (Microsoft - Cloud Solution Architect)
  - Tom Scavo (Internet2/InCommon)
- Central Time Zone
  - Walter Hoehn (U. Memphis)
  - Barry Ribbeck (Rice)
  - David Langenberg (U Chicago)
  - Scott Koranda (LIGO and SCG)
  - Paul Caskey (Internet2)
  - Tommy Doan (SMU)
  - Brett Bieber (U. Nebraska-Lincoln)
- Mountain Time Zone
  - Nick Roy (Internet2 T&I, Denver)
  - Nate Klingenstein (Internet2)
  - Janet Yarbrough (Aegis Identity)
- Pacific Time Zone (it's early on the West Coast!)
  - Judith Bush (OCLC, San Mateo office)
  - Andrew Hughes (Independent Consultant, Victoria, BC)
  - Eric Goodman (University of California)
  - Russell Beal (USC)
  - Dedra Chamberlin (Cirrus Identity)
- Other Time Zones

Agenda:

- Welcome
- Agenda Bash
- Overview of Charter, Goals, and Timeline
  - Clarify what interop means in this context -- consistent way to require behavior in the context of interaction between an IdP and SP in InCommon

Discussion 8/10/2015:

- Prioritization and categorization of work to be done in alignment with charter
  - Interop requirements for implementers
  - “” deployers
  - Policy issues
  - Site operational practices
  - Testability

- Scope of work for this group - what the charter asks, and notes as deliverables, vs. discussion on the list to date - what will be most useful? One driver is: feed stock for the future InCommon validation program for Internet2 Industry partners (f/k/a InCommon Affiliates).

Discussion:

- What should the output of this group look like?
  - No mention about how this work will pick up from other work in the past (vendor guidelines work from the past as potential starting place)
  - There have been some informal lists in the past, but this is the more long-term/thoughtful outcome of the ad-hoc work that was done very quickly a few weeks back
  - Scott Cantor mentioned: SAML Implementation Profile
  - Combination of sources: saml2int, older implementation work for InCommon a while back, etc. Expectation that aside from any best practices documentation, there would be a formal implementation profile that might be labeled InCommon or wider in scope, and hope for an update to saml2int.
  - Work needed for new version of saml2int
    - A number of years since published
    - A result of a fair amount of compromise
    - Doesn’t go far enough in certain areas/maybe goes too far in others
    - List of small edits that had been compiled by Kantara/no one to currently work on it
    - Some larger changes that have been suggested over time
    - Things have changed in 5 years / need for a refresh / may result in a larger set of changes.
  - How do we relate back to that (saml2int) work? If it’s a moving target or perhaps not what we want, do we build on top of that or try to push changes into it?
  - Not a moving target: No active work on it right now, we should try to push changes into it. Document is open to input.

- **AI: Scott Cantor will post** list of recommended changes for saml2int
- Rainer: GÉANT is looking at funding a similar effort, if that goes forward, we would have a good shot at bringing forward the work and integrating with test harness from Roland Hedberg (fedlab.org) [Try https://github.com/rohe/fedlab & https://fed-lab.org]
- Walter: Priority from TAC was the implementation profile, but when we took a census of what real problems people were having in the wild, it seemed like many were deployment, but kind of straddled the line ("what does my implementation allow").
- Scott C: Metadata support is the one area where there is a lot of problem if products don't support it. Saml2int is silent about metadata usage, and it's a deployment, not implementation, profile. Not used to motivate implementation changes on the part of products. You can't configure a deployment to do things an implementation doesn't support. Also interested in effectively replacing the OASIS SAML V2.0 Conformance document, there is no way to update it because it's part of the standard. It desperately needs to be updated, best way to do that is to come up with a list of requirements that can supersede it.
- Walter: Two work products could be:
- 1- Implementation profile (supplanting SAML 2 conformance document)
- 2- Set of recommendations that feed into saml2int - list of changes, or proposed replacement document
- Scott Koranda: Want to focus on research and scholarship service providers and their ability to interop with IdPs - wonder if this WG needs to recommend how the baseline practices for InC should change, even for sites that are using the most technically capable tooling, are there things that need to be done to address policy/etc related to default interop?
- Dedra Chamberlin: Good scope of group, but won't reach it's goals if campuses don't have business processes that promote interoperability. There may need to be an expansion of scope or a separate group. Try to change requirements of the federation so that default attribute release can happen in the future. Also keep finding out about vendor ops that support SAML, but haven't figured out what federation is all about. If we promote interoperable IdPs that release attributes, it will be easier for these types of vendors to realize the benefits of federation
- Walter: We can't leave those things out if our overall goal in higher ed is interoperable by default. "Simple things should be simple, hard things should be possible." We're trying to address the "Simple things should be simple." Things should just work for the basics, for some limited set of things. Biggest challenge: attribute release. Perhaps that's some InCommon or higher-ed-specific document on attribute release.
- Scott C: That's a difficult thing to take on for this WG: Advocacy for attribute release. It's difficult to convince IdPs to change - they want to be

invisible, they don't want to be part of the community. Their use cases are Box, O365, Google Apps, etc. The "hide from discovery" category that REFEDS has been working on, and all the Shibboleth discovery filtering have been focused on hiding those types of IdPs from discovery. The idea that we could get 2,000+ universities to play ball is pretty daunting.

- Gregory Katz: One of the charters for Microsoft is to work on interoperability. What are those needs that the research community has in US. Would hope that we could get some info from this group on how to provide that value.
- Scott K: Hide from discovery: Should this group ask InCommon to make changes to make it easier to use that category - should InCommon be applying that label directly to the "known non-interoperable IdPs"? The metadata labels for MDUI - should InCommon require them?
- Scott C: I think those things are appropriate, short of "how does InCommon convince 1,000 IdPs to release attributes?"
- Russ Beal: I think we have a bit of an education thing, too, did not even know I could configure the "hide from discovery" metadata element in the Federation Manager. Would want to let people know about this if they can do it themselves. *Note*: It is not currently possible to self-declare the hide-from-discovery entity attribute in the Federation Manager.
- Scott C: Dedra made a good point, but very hard: How do you get a bunch of vendors to care about something if you aren't willing to exert your own voice/force on the issue. It wasn't paying off to get people to try to pay attention to this stuff.
- Dedra: If things were just very clearly spelled out to the vendors, it would be great, but it hasn't worked. The documentation is there. "Here is how you support federation in your product and why it's important to you." - shouldn't be part of this group, *but to have the work of this WG have more impact, some other effort should be made to craft stories for vendors about why this will help you.* Seeing a lot of smaller vendors in the edtech space who are trying to sell into higher ed, but they don't get federation, could use persuasion in language that makes sense to them.
- Walter: There is benefit in speaking with one voice, not sure that has been done on the full range of issues that we might tackle. Multiple vendors that care enough to be on this call.
- Nick: Background on why this group was chartered: More refined set of minimum implementation and deployment requirements, and testables for interoperability in the context of InCommon.
- Walter: Summary: Clarity: items that go into saml2int and an implementation profile. Less clear: Other things that might feed into higher ed spec, best practices, questions to raise with InCommon to spin

off other groups, etc. How do we prioritize our work? First focus or splitting up into subgroups?
        - Barry: Seeing a diversion - charter specifically asks what, not how. And specifically w/r/t to communication between SAML implementers and deployers and InCommon. That work could be fairly straightforward, but beyond that it would be very challenging.
        - Rainer: Looking into current implementation from Kantara/saml2int - how to take these documents as a starting point. That's a baseline for a number of e. government initiatives - will come up with a proposal within a week or so.
        - Scott K: One of the work products of this group should be to develop a list of things that we want InCommon to require of its participants to promote interoperability, because it is specifically listed as item number four (4) on the charter.
        - **AI: Walter Work with Nick** to try to summarize some of the discussion we've had thus far and map that into a plan for next week's call. Some areas where there is consensus on what we should do. Once we write up those, will ask for volunteers on the list to begin collating items related to those work products.
    - Summary of discussion on the list so far. Some common themes:
        - Service design and integration are often seen as problems which are more difficult than the mechanics of SAML implementation and metadata consumption, but possibly not ones that we can address within InCommon. "We are the only market that asks for more than the least common denominator."
        - Consistent behavior with regard to metadata use/consumption is a significant challenge
        - Classes of deployment-time issues - bi-directional (IdPs on SPs, SPs on IdPs) - some examples: attribute release, attribute definitions, attribute values, identifiers, contracts, privacy/opacity/pseudonymitiy vs. immutability and identifiability, deep-linking URLs that require login from a specific IdP
        - Classes of SAML implementation issues - multilateral signed metadata consumption, validation, reloading; Correct handling of AuthN context; Handling of encrypted assertions; Support for SP-initiated SSO; Use of the SAML 2 Web Browser SSO profile / saml2int; Support for key rollover; Support for long-lived self-signed signing and encryption keys in metadata

- Discuss proposed sub-groups and parallel efforts
- Open discussion
    - See list of resources available on WG wiki space.