Scribing Document Archive

MFA Interoperability Profile Working Group - Scribing Document

- Back to the wiki for this working grou

Short URL for this document: https://goo.gl/0XREgl

- Open Document download of the original Google Doc: MFAInteroperabilityScribingWGDoc.odt

Dial-in numbers:

+1-734-615-7474 (Please use if you do not pay for Long Distance)

+1-866-411-0013 (English I2, toll free US/Canada Only)

PIN: 0148636#

NOTE WELL: All Internet2 Activities are governed by the Internet2 Intellectual Property Framework.

Index to Meeting Notes

Work Group Call - August 25, 2016

Attendees

- David Walker, InCommon/Internet2
- Karen Herrington, Virginia Tech
- Mark “Max” Miller, Penn State
- Tommy Doan, Southern Methodist University
- Roger Safian, Northwestern University
- Phil Pishioneri, Penn State
- Jim Jokl (late), Virginia

Agenda and Notes

- Final Products of the MFA Interoperability Profile Working Group
  - The group decided to accept our products for final submission. The AAC’s request to incorporate Brett Bieber’s edits to MFA Technologies, Threats, and Usage was already done.
- Issues Identified after Completion of the Final Report
  - We talked about Eric’s comment on MFA Technologies, Threats, and Usage to clarify that verifying password and second factor separately in the IdP is OK. The wording could be clearer, but it’s correct, so we decided to leave it as is.

- Congratulations, everyone! We did a great job! If you're going to TechEx, please come to our session on Monday, 9/26/16, 10:20AM-11:10AM (https://meetings.internet2.edu/2016-technology-exchange/detail/10004357/). There was also talk of meeting for a celebratory drink...

Work Group Call - June 9, 2016

Attendees

- Karen Herrington, Virginia Tech
- Mark "Max" Miller, Penn State -- Let's Go Pens!
- Eric Goodman, University of California -- Let's Go Dubs!
- David Langenberg, UChicago
- Roger Safian, Northwestern University
- Scott Cantor - tOSU - just shut up about your damn teams (unless it's College Football)
- Tommy Doan - Southern Methodist University

Agenda and Notes

1. Welcome
2. Agenda bash
3. InCommon MFA Profile
    a. No changes. Considered "final" (with concerns about wording of the URI… "incommon" and "assurance")
4. InCommon Base Level Profile
    a. Changes accepted. Considered "final" (with concerns about wording of the URI… "incommon" and "assurance")
5. MFA Profile Usage Guidance
    a. Changes accepted (changes were last made on the previous call). Considered "final"
6. Final Report of the MFA Interoperability Profile Working Group
    a. Appears to be missing the following:
        i. Discussion of Entity Attribute, and distinction between "MFA" entity attribute and the alternate "authncontexts_supported" entity attribute discussed at June 2 meeting
        ii. New "stronger authn" group charter
            1. Concern that this group might go "too far" and over-prescribe (InCommon Gold/Platinum)
            2. Perhaps approval of charter should be based on number of (existence of) SPs for which this is a real concern.
7. MFA Threats and Usage Document
    a. Volunteers (at least Eric) will look over and raise comments if any inconsistencies with subsequent work is found. Otherwise we will consider "final".
8. MFA Use Cases and MFA Use Case Descriptions
    a. Volunteers (at least Karen) will look over and raise comments too.
9. Karen will contact Nicole to see about submission for REFEDS consideration once the above changes are made.

Work Group Call - June 2, 2016

Attendees

- Karen Herrington, Virginia Tech
- David Walker, Internet2
- David Langenberg, University of Chicago
- Brendan Bellina, UCLA
- Eric Goodman, University of California
- Scott Cantor, tOSU
- Roger Safian, Northwestern
- Tommy Doan, Southern Methodist University

Agenda and Notes

1. Welcome
2. Agenda bash
3. Status of the possibility of a REFEDS consultation (Scott)
    a. There doesn't seem to be a light-weight process that would get us a URI to use for the profiles. We'll have to go with the full Consultation process.
4. Draft Charter for a Strong Identity Proofing Profile Working Group
    a. Please look it over for discussion next week.
5. MFA Profile Usage Guidance
    a. Eric will accept all of Scott's comments and call it done.
6. Proposed changes for the next revision of Final Report of the MFA Interoperability Profile Working Group and the profiles
    a. What should we do about the profiles' URIs?
        i. We'll pursue REFEDS consultation and consider an InCommon-only interim if it looks like that will take too long.
        ii. Karen and David will talk with Ann about bringing this to REFEDS.
7. InCommon MFA Support Entity Category
    a. Scott: This is an Entity Attribute, not an Entity Category.
        i. David will correct this. [Added to notes after the call. - DHW]
    b. Scott: Should we just define a metadata element that lists the authnContexts that the IdP supports?
        i. This satisfies purposes 1 and 3 in the draft spec. It's questionable whether 2 needs anything, anyway, since SAML says you can't lie in your assertions.
        ii. "Support" would mean something like "would reply successfully for at least one person"
        iii. Consensus on the call was that this is a good idea that's extensible to future profiles without inventing new entity attributes, however...
    c. The benefit of any flagging is marginal. Should we do anything?
        i. Consensus on the call was no.
        ii. Leave the decision up to the AAC by providing the draft entity attribute definition, but recommend it not be used.
        iii. Discussion will continue next week. Karen and David will discuss, too, and recommend a resolution.

Work Group Call - May 12, 2016

Attendees

- Karen Herrington, Virginia Tech
- David Walker, Internet2
- Roger Safian, Northwestern University
- Eric Goodman, University of California
- Scott Cantor, tOSU
- Paul Caskey, Internet2
- Eskil Swahn, SWAMID / Lund University

Agenda and Notes

1. Welcome
2. Agenda bash
3. No call next week?
4. Recommendation for next steps
    a. Propose as a REFEDS profile
        i. Scott Cantor will check with Nicole Harris about process. We may want to ask for a REFEDS URI, if approval of the profile would take a while.
    b. Create group to create "strong identification/registration" profile
        i. The new 800-63-3 should be considered in this work.
        ii. We'll recommend that the current group be rechartered (and perhaps renamed) to continue the work.

    c. Encourage adoption
        i. Incentives to use MFA in popular services (e.g., CILogon, Certificate Manager)
        ii. Communications campaign
        iii. Encourage people to contribute ways they address the “VOIP” and other deployment issues
5. Eric’s proposed edits for the Usage Guidance
    a. Everyone please review Eric’s proposed changes, particularly with respect to AuthnContextClassRefs he calls out.
    b. In general, we should review the document to make sure the language doesn’t sound normative, as opposed to guidance.
6. Public comments: Entity categories revisited
    a. Comments from Dean Woodbeck - 2016-05-11
    b. Comments from Jim Basney - 2016-05-04
        i. We’ll make our final decision on this in our next call. David will draft a spec to help the discussion.

Work Group Call - May 5, 2016

Attendees

- Karen Herrington, Virginia Tech
- David Walker, Internet2
- David Langenberg, uchicago
- Eric Goodman, University of California
- Scott Cantor, tOSU
- Paul Caskey, Internet2
- Chris Bahrami, Duo Security
- Roger Safian - Northwestern University
- Mark “Max” Miller, Penn State
- Eskil Swahn, SWAMID / Lund University

Agenda and Notes

1. Welcome
2. Agenda bash
3. Who’s going to Global Summit?
4. Public comments: Entity categories revisited
    a. Comments from Jim Basney - 2016-05-04
        i. Issues are filtering discovery, IdPs that “trap” the user and not return an error to the SP, and IdPs that crash.
        ii. Currently, InCommon would have to modify the Federation Manager to enable an MFA entity category, and IdP administrators would need to check the box.
            1. This applies to each federation in eduGAIN.
        iii. The long-term issue is that we’re likely to create a lot of entity categories, and people won’t understand how to use all of them.
            1. => We should recommend some future study of this issue.
        iv. Eskil : I would say that it is a key point in the ability for one university to trust another university’s MFA that it is marked by the Federation (and for example involves some sort of certification and for example prohibits incorrect onboarding processes)
            1. SWAMID will be defining an entity category for this. Would be useful to link to their documentation when it becomes more ready for comment/sharing.
        v. The discovery use case is probably the most important.
            1. How many SPs will require federated MFA, as opposed to asking for it and providing their own MFA if the IdP does not provide it?
        vi. Criteria for an entity category
            1. “Support” MFA profile
                a. Assert for at least one person? (See R&S discussion of “some population”)
                b. IdP does not “trap” users, but returns error to SP (or another requested context) (Is this specific to “if the user does not have MFA registered”? Many IdPs trap users under PPT use cases.)
                    i. Our scope is MFA, so this would apply only to MFA.
                    ii. What is “our scope” if a request includes /mfa OR /ppt (/mfa preferred)?
                    iii. => We won’t require this.
                c. Does it have any implication that campus administration has “signed off” on it?
                d. Include Base Level profile somehow? For all users?
            2. Concern about defining an entity category that is used to infer behavior beyond what the formal definition states.
                a. E.g., using it to determine that the IdP can process arbitrary RequestedContexts without crashing (non-mfa specific)

Ran out of time at this point...

1. Recommendation for next steps
    a. Propose as a REFEDS profile
    b. Create group to create “strong identification/registration” profile
    c. Encourage adoption

        i. Incentives to use MFA in popular services (e.g., CILogon, Certificate Manager)
        ii. Communications campaign
        iii. ???
    d. ???

Work Group Call - April 28, 2016

Attendees

- Karen Herrington, Virginia Tech
- David Walker, Internet2
- Brett Bieber, University of Nebraska-Lincoln
- Roger Safian, Northwestern University
- David Langenberg, University of Chicago
- Mark “Max” Miller, Penn State
- Eric Goodman, University of California
- Mike Grady, Unicon
- Mary Dunker (Virginia Tech)
- Scott Cantor, tOSU
- Chris Bahrami, Duo
- Eskil Swahn, SWAMID / Lund University

Agenda and Notes

1. Welcome
2. Agenda bash
3. Public Comment Threads received to date from assurance@lists.incommon.org
    a. Please add any additional comments you’d like prior to the call.

- Tom Barton’s comments
    - Do we want to say more about the MFA technologies and threats document, in particular what our process was for determining the information there.
        - “Reflects consensus and knowledge of the group” for additional information Cohortium, 800-63, AuthN Whitepaper (referenced by Cohortium), etc.
        - Any references to 800-63 or the like that are valid?
        - Possibly not worth “making up” references.
    - The comment in the guidance paper about registration practices…
        - “...no more secure than using the initial password on its own”
    - Comment about second factors protected by the first factor
        - Give an example of an insecure use.
        - Possible to use language like suggested above (“no more secure than…”)
        - We decided to be silent about possible misinterpretations of two different factors vs. two different types of factors.
        - Mike Grady observed that the use cases they’re seeing at Unicon are within an enterprise, and controlled on the IdP side.
            - We’ll talk about this in the next agenda item.
- Allan Kim’s comments
    - We’ll add advice in the guidance document for SP administrators to check the assertions they receive to ensure they’re what is required.

1. Recommendation for next steps
    a. Propose as a REFEDS profile
    b. Create group to create “strong identification/registration” profile
    c. Encourage adoption
        i. Incentives to use MFA in popular services (e.g., CILogon, Certificate Manager)
        ii. Communications campaign
        iii. ???
    d. ???

- We tossed around some ideas, but we’ll continue this discussion next week. Mike will contact Jim Basney about CILogon, and others are encouraged to reach out to potential use cases.

Work Group Call - April 14, 2016

Attendees

- Karen Herrington, Virginia Tech
- David Walker, Internet2
- Brett Bieber, University of Nebraska-Lincoln
- David Bantz, U Alaska
- Mark “Max” Miller, Penn State Penguin Fan
- Phil Pishioneri, Penn State Ditto ^
- Scott Cantor, tOSU
- Eric Goodman, Warriors Fan and University of California
- Chris Bahrami, Duo Security
- Paul Caskey, Internet2
- Roger Safian, Northwestern University
- Eskil Swahn, SWAMID / Lund University

Agenda and Notes

1. Welcome
2. Agenda bash
3. Documents for Public Comment
    a. We will place our documents here after this call for inclusion in the TIER version 1 announcement.
    b. Call for comments by May 16.
4. Final review of our documents before opening for community comment
    a. InCommon MFA Profile
        i. We reworded the bullet about independent factors.
    b. InCommon Base Level Profile
        i. We left the language that says the session has been authenticated, not necessarily the user.
    c. Multi-Factor Authentication (MFA) Interoperability Profile Working Group Final Report
        i. Everyone, last chance for comments is Friday (4/15) morning (Eastern).
    d. MFA Profile Usage Guidance
        i. Scott made a number of edits to firm up SAML-related issues.
        ii. Last chance for comments is Friday (4/15) morning (Pacfic).
    e. MFA Technologies, Threats, and Usage
        i. No changes
    f. Note that we are not finalizing these documents right now, only opening them for community comment.
        i. David will export the profiles and MFA Technologies, Threats, and Usage to Documents for Public Comment today. The other two documents will be exported tomorrow afternoon (Pacific) after he gets OKs from Karen and Eric.

=> There will be no call next week.

Work Group Call - April 7, 2016

Attendees

- Karen Herrington, Virginia Tech
- David Walker, Internet2
- David Langenberg, UChicago
- Eskil Swahn, SWAMID / Lund University
- Brett Bieber, University of Nebraska-Lincoln
- Scott Cantor, tOSU
- Mary Dunker, Virginia Tech
- Paul Caskey - Internet2

Agenda and Notes

1. Welcome

2. Agenda bash
3. Let's try to be ready for public comment after next week's call.
    a. Review final report next week.
    b. TIER v1 release is April 16.
4. MFA Profile Usage Guidance
    a. Please review and comment before the call.
    b. Do we have the right names for the profiles?
        i. How about "InCommon Base Level" and "InCommon MFA"? Yes.
    c. We won't modify the normative text to indicate "persistent" threats, as opposed to short-term.
    d. We'll keep offline cracking and online guessing on the same bullet.
    e. Is a phone number acceptable as a second factor?
        i. Yes, if it's not authenticated (only) with a password.
        ii. It's acceptable for an enterprise to mitigate bypass of this by end-users through policy, education, and enforcement.
        iii. The usage guidance will indicate these things. No change to the profile is needed.
    f. Should re-registration be required to require both factors (or not just first factor)?
        i. We'll want to add concepts of "independence of factors" to profile, as well as controls for re-registration. Eric will propose wording.
    g. We won't include a section about a factors that are not directly verified by the IdP (e.g., a password-protected X.509 cert). They're allowed in our profile.
    h. Scott suggested some cleanup of SAML-specific language.
5. We ran out of time at this point. Watch for potential announcement of an additional call...
6. Issues for the Profiles
    a. Walter's clarifying language about session length
    b. Should we add a comment that a factor (e.g., a VOIP service) that's unlocked with a password is not distinct from username/password?

Work Group Call - March 31, 2016

Attendees

- Karen Herrington, Virginia Tech
- Nick Roy, Internet2
- Walter Hoehn, Memphis
- Brett Bieber, U. Nebraska-Lincoln
- Eric Goodman, University of California
- Scott Cantor, tOSU
- Mary Dunker, Va Tech
- Eskil Swahn, SWAMID / Lund University
- Paul Caskey, Internet2

Agenda and Notes

1. Welcome
2. Agenda bash
3. MFA Profile Usage Guidance
    a. Are there issues that should be moved to the profiles?
        i. EricG: Everyone should review, and if there are things we all agree on, then they should probably be moved into the profile.
        ii. AI: Full group look through guidance on call, work through it, find issues - EricG walk us through it.
        iii. There is overlap between this and Jim Jokl's matrix, and that's good. How much detail here is useful?
        iv. Should we wordsmith 'a persistent threat to user authentication' back into the MFA profile?
        v. Discussion of being normative vs. not - being very prescriptive is difficult (see: Assurance program), but some of this needs to be an absolute requirement, or it's not worth doing.
        vi. Hot button issue: any second factor which is accessible via a first factor should be explicitly called out as something that is not acceptable.
        vii. Consensus: Anything that's a MUST must be put into the profile
        viii. SHOULD doesn't mean anything in a spec
        ix. Might want to include accessibility considerations in the guidance
        x. Discussion of SAML flow guidance - may not want to put shibboleth-specific material/examples in this section.
        xi. Not valuable to put something in the guidance unless it refers to a normative requirement of the profile? Not helpful to give advice the IdP can't do anything with.
        xii. Should take out guidance on trusted devices unless they are explicitly forbidden by the profile. Profile says 'user's current session' - that needs to get strengthened/clarified in the profile.
        xiii. AI: Walter will propose new language for the profile about what it means to have done MFA in the context of the user's current session.
    b. Should this be discussed in next week's Assurance Implementers call?
        i. Mention that we're working on this, but don't explicitly share it yet until we're out of heavy drafting mode.
        ii. Will be open to community review of the profiles/guidance when they're out of draft.
4. InCommon Base Level Profile
    a. Should this have a criteria to comply with the Participation Agreement?
    b. Should this not be InCommon centric to enable use by other federations?
        i. These two things are diametrically opposed
        ii. Proposal - this is a 'null' profile that you get to ask for, and it should be nothing more. That would allow it to be useful to other federations.

iii. If it's explicitly unspecified, that means deployers asking for 'base level' you don't get to see, e.g. passwordProtectedTransport
iv. If you allow 'anything' - you could get back ip-based or other really weak authN, and you would not know.
v. If you rule something out, it's no longer base-level.
vi. Eric will capture this distinction in the usage guidance, for now.
1. Do we really need three profiles? (that was mostly intended to be facetious)
a. Null
b. Wrapper for password protected transport (or - just not 'really bad authentication - like IP-based')
c. MFA base profile

5. Status of final report
a. Karen has started on it
6. Other items
a. Brett - prepare ourselves for moving this to REFEDS?
i. David, Ann and Nick discussed. Yes, likely should take to REFEDS for review/etc.
ii. REFEDs recent discussion for SIRTFI seems somewhat analogous and so could be a good approach to take.
iii. nicole.harris@geant.org - may want to contact ahead of time to bounce ideas off her/get her take.

Work Group Call - March 24, 2016

Attendees

- Karen Herrington, Virginia Tech
- David Walker, Internet2
- Roger Safian, Northwestern University
- Scott Bradner, Harvard U.
- David Langenberg, uChicago
- Tommy Doan, Southern Methodist University
- Scott Cantor, tOSU
- Jim Jokl, Virginia
- Nick Roy, Internet2
- Brett Bieber, University of Nebraska-Lincoln
- Eric Goodman, University of California
- Walter Hoehn, Memphis
- Paul Caskey, Internet2

Agenda and Notes

1. Welcome
2. Agenda bash
3. Complete language for our profiles, based on comments received during the week
a. InCommon Base Level Multi-Factor Authentication Profile
i. We're editing and resolving comments.
ii. After review of the usage guide, we'll consider if some of its issues should move into the profile
1. In particular, the issue Walter raised about whether Duo's "trusted devices" are allowed.
2. David mentioned that Duo will be asked to review what we've done, probably recommend configurations that comply. (Nick Lewis, who has Duo in his Net+ portfolio, knows about this and participates in our group.)
iii. We got through the document and resolved all comments (for now, at least).
b. InCommon Base Level Profile
i. We resolved all comments, except for whether we should have any criteria for this profile. What's there doesn't require anything other than InCommon membership, but maybe we should have nothing at all.
ii. We'll continue this discussion next week.
4. MFA Technologies, Threats, and Usage
a. This document is complete.
5. MFA Profile Usage Guidance
a. Everyone is asked to read and comment on Eric's draft for discussion next week.
6. If there's time, brainstorm an outline for our report
a. There was not enough time.

Work Group Call - March 17, 2016

Attendees

- Karen Herrington, Virginia Tech
- David Walker, Internet2
- Scott Bradner harvard university
- Eric Goodman, University of California
- Roger Safian, Northwestern University
- Nick Lewis - Internet2
- Jim Jokl - Virginia
- Chris Marron - University of Central Florida
- David Bantz, U Alaska
- Ayesha Benjamin - University of Central Florida
- Tommy Doan, Southern Methodist University
- MIke Grady, Unicon
- Eskil Swahn, SWAMID/Lund University
- Scott Cantor, tOSU
- Brett Bieber, Nebraska

Agenda and Notes

1. Welcome
2. Agenda bash
3. Review of our Use Cases
    - Is our authentication-only profile good enough for anyone's use cases?
        i. Good enough for Brett Bieber (U Nebraska) for the student information system, shared with state colleges.
        ii. Same for Eric Goodman (U California), except that it's a new HR system. And may be context specific (i.e., what the user is doing, rather than who the user is).
        iii. Very similar to one of our main use cases in SWAMID, although we have one upcoming student documentation system and about 35+ members that need to implement MFA for the staff
    - Discussion of issues related to whether services need MFA all the time, or if they may need it later, depending on what the user does. In the first case, the SP just requests MFA. In the latter the SP may request only non-MFA initially, and MFA later, or it may request either MFA or non-MFA initially (and then require it later).
4. MFA Technologies, Threats, and Usage
        i. [I'm still unclear on difference between static and dynamic Phishing - matters most for Duo push]
        ii. Are we trying to require mitigation of the user bypassing authentication processes (e.g., configuring your voicemail to respond to Duo requests)?
            1. It needs to be included in security awareness training.
        iii. What phones are allowed? Not VOIP that authenticates with a password. Phone number should be tied to a specific outlet or device (cell phone).
            1. The IdP/institution will have to have a process to figure this out
5. Complete language in the profiles
    - InCommon Base Level Multi-Factor Authentication Profile
        i. Is it OK for one of the two factors to be verified at two different times?
        ii. Security training requirements (only if voice allowed?)
        iii. What is allowed technology-wise (table 1 of threats page)
        iv. No Enterprise [phones/devices/factors] if accessible (solely) via same password/credential as IdP authN
    - InCommon Base Level Profile

Work Group Call - March 10, 2016

Attendees

- Karen Herrington, Virginia Tech
- David Walker, Internet2
- Brett Bieber, U. of Nebraska-Lincoln
- Scott Bradner, Harvard U.
- David Bantz, U Alaska
- Mike Grady, Unicon
- Mark "Max" Miller, Penn State
- Scott Cantor, tOSU
- Tommy Doan, Southern Methodist University
- Eskil Swahn, SWAMID / Lund University
- Eric Goodman, University of California
- Nick Roy, InCommon/Internet2
- Phil Pishioneri, Penn State

- David Langenberg, uchicago
- Rob Pierce, Sewanee
- Mary Dunker, VA Tech (joined call late)

Agenda and Notes

1. Welcome
2. Agenda bash
3. Plea for use cases descriptions
    - At least, do you see our base-level MFA profile as being good enough for your use case?
    - InCommon has been having internal discussions of the use of this profile for the Certificate Manager and Federation Manager. Paul is consulting with Comodo for the Certificate Manager. The thinking for the Federation Manager is that stronger registration practices would be needed in conjunction with our base-level MFA profile.
    - Since we have problems getting complete use cases I paste two scenarios I wrote about last June just to get something written:
        i. 1. SPs with high security needs where the SP would like encapsulate the entire login session behind MFA authentication. An example here would be a login handler to Shibboleth available to SPs by the use of a specified AuthContext. Rather transparent to the SPs which need only to request the specific AuthContext.
        ii. 2. SPs with high security needs for specific functionality. An example here would be an SP which use normal user credentials (ePPN/password for example) to allow initial access to the SP and then need to verify the user with a higher certainty when the users uses certain functionality. To clarify, you could for example have an SP which allow users to browse invoices by logging in with normal credentials but the SP would have application based functionality to verify a MFA based credential (through for example a web service) if the users actually want to sign off one of the invoices. Also fairly easy to implement technically but with the drawback that you need specific application based logic to handle every case. Perhaps not an issue in self-developed webb applications but a bit tougher to expect normal vendors to implement.
4. Please read Jim Jokl's MFA Technologies, Threats, and Usage for discussion next week.
5. Finalize InCommon Base Level Multi-Factor Authentication Profile for public comment.
    - Do we want to address the issue of defining a base-level profile for anything that's acceptable to the federation or leave it for future work? InCommon Base Level Profile is a first pass at that, but we should decide if it's valuable before spending more time on it.

- There was some discussion of the success and failure of different assurance programs in SWAMID, InCommon, and UCTrust… InCommon hasn't had a big take on Silver and Bronze. Our effort is an attempt to address more specific needs of relying parties.

	Low Security	High Security
Assurance Level 1	WiFi-login	"Facebook MFA"
Assurance Level 2	Normal login to a university system	Login to invoice system/student administration

What I meant to illustrate is that we view MFA as something different than Assurance Levels. "Facebook MFA" is something that we so far haven't found a need for. This is for private "consumers" which value their Facebook accounts. The good thing is that we on the other hand see a high value of aligning the discussions and use the same MFA profile if possible (and of course provide this as a part of the official Shibboleth IdP branch)

- There was consensus that we don't want any certification.
- We discussed an entity category that indicates that an IdP supports the MFA base-level profile. Also, perhaps, that an SP will respond appropriately to errors in the MFA authentication process.
    - Defer for future work (when we have more understanding of what's needed.)
    - For now, multiple authentication requests can probably handle use cases, but may not be optimal.
    - It may be useful for reporting, e.g., how many IdPs support MFA.
        - => We'll put this in our report for InCommon to do.

Work Group Call - March 3, 2016

Attendees

- Karen Herrington, Virginia Tech
- David Walker, Internet2
- Scott Bradner, Harvard
- Scott Cantor, tOSU
- Tommy Doan, Southern Methodist University
- Ayesha Benjamin, UCF
- Eskil Swahn, SWAMID/Lund University
- Jim Jokl, Virginia
- Brett Bieber, University of Nebraska-Lincoln
- Eric Goodman, University of California
- Mary Dunker, Virginia Tech

Agenda and Notes

- Welcome
- Agenda bash
- Review of our MFA Use Case Descriptions (see assignments below).
    - We'll generalize the WorkDay description to cover other enterprise applications with varying riskiness of transactions.
    - Eric has offered to add some Univeristy of California cases.
    - Brett (Nebraska) will add to the Intra-campus use cases
- Review of our Example Base-Level MFA Technologies (see below).
    - Duo has many options. We may want to provide some guidance of which are compliant this our spec.
    - Jim offered to expand on the material here.
- Review of our DRAFT Base-Level MFA Profile.
    - Eric: We should define the authentication context, then talk about the compliance issues.
    - Scott: The formal definition should include the schema. He can do this.
    - Jim: Should we say something about identity proofing (even if it's the "base" "we use this for ourselves")
        - We could add that to higher-layered profiles
        - We should consider a base-level (not MFA) profile that this layers on top of.
        - Can address at least some of this in the usage notes.
        - General agreement that this is out of scope for this profile (but not future profiles)
        - Scott: Advocates not having ANY proofing requirement. Brett, Mary, Karen concur. Brett: This profile is entirely about enhancing the authentication mechanism.
            - Scott's experience is that "proofing" typically happens at the application, and that the application typically only wants the authncontext to manage identifier repeatability.
        - Later discussed whether "registration" needs to be have criteria as well.
            - At the least we need to clearly define "proofing" vs. "registration" so we can distinguish what we're trying to constrain.
    - Move definition of the authentication context to a new definition section, then reference the definition in the compliance section.
        - Reference the 800-63 language of multi-factor.
    - Certification
        - Institutions (via their executive contact?) will self-certify that their IdP asserts the profile correctly.
- Process for community review.
    - We'll plan to solicit community review of the draft profile, use cases, and target technologies after next week's call.

Work Group Call - February 25, 2016

Attendees

- David Walker, Internet2
- Karen Herrington, Virginia Tech
- Scott Bradner, Harvard U
- Roger Safian, Northwestern University
- Scott Cantor, tOSU
- Tommy Doan, Southern Methodist University
- Eric Goodman, University of California
- Eskil Swahn, SWAMID/Lund University
- Helen Fankhauser, Univ of NE
- Mark "Max" Miller, Penn State
- Phil Pishioneri, Penn State
- Brendan Bellina, UCLA
- Jim Jokl, Virginia
- David Langenberg, UChicago
- David Bantz, U Alaska

Agenda and Notes

- Welcome
  - KH: Want to refocus on our charge. Have short timeline, so need to stay focused.
- Agenda bash
- Review of our charge
  - (We don't have a lot of time…)
  - "The mission of the working group is to develop and document requirements for creating and implementing an interoperability profile to allow the community to leverage MFA provided by an InCommon Identity Provider by allowing SPs to rely on a standard syntax and semantics regarding MFA."
  - Deliverables
    i. Assemble use cases that will motivate the deliverables of this working group
    ii. Develop short list of widely deployed MFA technologies in higher education that will be in scope for the profile
    iii. Define requirements for and draft MFA Interoperability Profile
    iv. Develop and recommend scope and plan for adoption
    v. Present draft to InCommon community for review
    vi. Publish final profile
  - Principles
    i. Profile should be constrained to address the articulated need for distributed MFA.
    ii. Ability to implement with current MFA and Federation technology should be a core design constraint.
    iii. Support for this capability should be exposed in the Federation Metadata.
  - Proposal: Limit ourselves to federated use cases and SAML. Don't worry (too much) about incomplete SAML implementations.
    i. One of the interesting use cases is WorkDay. It's not clear they're interested in federating.
      - We'll include SaaS in our scope, independent of whether WorkDay is specifically interested
    ii. What we do will be useful outside of SAML, but we'll focus on SAML.
- Assign people to write a few sentences for our MFA Use Cases. Here's the list from our last call:
  - InCommon Certificate Manager (Paul/Nick Roy/Comodo)
  - Federation Manager (Paul/Nick Roy)
  - WorkDay
    i. Use SAML MFA for WorkDay
  - LIGO (Scott Koranda)
  - Federal services (FICAM, Paul)
  - Intra-campus use cases (Dave Langenberg)
  - Federated AuthN to a single Grouper instance (Keith)
  - The few sentences should just describe the use cases. You don't need to discuss implications of the use cases at this point (although it' s OK if you want to).
- Create the "short list of widely deployed MFA technologies"
  - Can we get a few volunteers to do this for next week?
  - E.g., smart phone app, key fob, …
    i. http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf as background? (Their "categories")
  - We'll post a place where people can contribute ideas, and Karen and I will summarize and/or augment on Wednesday for next Thursday' s call.
- Define what we mean by MFA
  - We may not decide this is strong enough, but it will serve as a baseline.
  - Some possibilities
    i. From Paul: "When SAML Authentication Context 'xyz' is used in a SAML Authentication Request or subsequent SAML Authentication Response, the meaning of that value is that a discrete second factor will always be (or was) used in the initial authentication event for the current web SSO session. Such second factor will be resistant to phishing attempts and will be used regardless of the user's device or location. Normal SSO session options (duration, etc) are allowed."
    ii. Inspired by How Much Security Is Enough? (replacing the bolded sentence above): "The combination of first and second factors must mitigate first-factor-only risks of phishing, offline cracking, and online guessing."
      - This doesn't eliminate, e.g., offline cracking, but it means that a cracked password isn't enough to authenticate.
      - Do we care if both factors are validated in the same process (a hardware PKI token that requires a PIN), or at different times (username/password + Duo or U2F)? - No, but we may care for profiles that are stronger than the baseline.
        - This is probably true for man-in-the-middle, too (even in the context of websso??).
          - What resistance should the websso have? man in the middle, session hijack (perhaps more from the 800-63 list)
          - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf
      - We'll go with this sentence.
      - We need a normative statement that expresses the requirement, then we can talk about examples, etc., of what would comply. If in two documents, they should reference each other.
      - We also need information on the registration process; +1
        - Must mitigate the risk that the two factors were assigned to two different people.
      - Eskil: I believe it is important that the second factor should be resistant to phishing, offline etc in itself. The first sentence was in my opinion a stronger wording regarding this.
      - Addition to Use Case homework: Is the base-level definition of MFA sufficient, or do we need some more of these other things in the base level?
  - Does this address our use cases? What else do we need to add to address more use cases? Should those things be added in additional profiles?
- Karen and David will draft a strawman base-level profile for discussion next week.

Attendees

- David Walker, Internet2
- Karen Herrington, Virginia Tech
- Brad Schwoerer, University of Wisconsin-Whitewater
- John Fontana, Identity Evangelist, Yubico
- Jeffrey Williams, Identity Management Engineer, UNC-Greensboro
- David Langenberg, University of Chicago
- Scott Koranda, LIGO
- Scott Cantor, tOSU
- Nick Lewis, Internet2
- Brett Bieber, University of Nebraska-Lincoln
- Paul Caskey, Internet2
- Tommy Doan, Southern Methodist University
- Scott Bradner, Harvard U.
- Eskil Swahn, SWAMID / Lund University
- Mary Dunker, Virginia Tech
- Eric Goodman, University of California
- Keith Hazelton, UW-Madison
- Mark “Max” Miller, Penn State
- Jim Jokl - Virginia
- Robert Gorrell, UNC-Greensboro
- Ayesha Benjamin, University of Central Florida
- Brendan Bellina, UCLA
- Roger Safian, Northwestern University

Agenda and Notes

1. Welcome
    - Karen: We need to
2. Agenda bash
3. FYI: GTRI Trustmark Pilot. Specific trustmark definitions are at https://trustmark.gtri.gatech.edu/operational-pilot/trustmark-definitions/
    - Trustmark Definition (TD): Implementation of Multi-Factor Hardware Cryptographic Tokens is a good example.
    - Discussion of scope:
        - Scott C: Is signaling in scope or are we just focused on what (technology/product) would meet the MFA/strong authN criteria?
            - Paul: Some “yes” statements, signaling is in scope
            - Presumption/statement that the base level signaling will be via AuthN context
        - Scott C: Registration processes were discussed as being potentially out of scope for us (separate requirement to be addressed later), and that may lead to a lack of universality for these solutions.
            - Draws a strict line around what is being defined, and that means that some people will find this insufficient.
        - Mary: Is the focus on defining “strength” of MFA or is that the assurance group?
        - Jim: If the requirement of the MFA is to avoid Phishing (or whatever the “correct” term is…) then it may be distinct from LoA
            - “Registration of a second factor must be done through a mechanism that is Phishing resistant”
            - Paul (and others): talking about initial registration having a window of availability.
            - Scott C: referred back to VOIP vs. registration (specifically, doesn’t VOIP undermine any claim that second-device reg. require a non-phishable factor?)
        - Everyone agrees that “good registration” is important but how detailed to specify the requirement or whether to punt it is the question (and the thing that’s difficult to define clearly).
        - We agreed that we can amend this profile and add more profiles in the future.
            - Eric: whether to solve by adding more profiles vs. trustmarks or attributes that modify the existing profiles can probably (or at least pragmatically must…) be deferred.

As an example Lund University is implementing the bootstrapping of a second factor (in the first wave Google authenticator) like this:

1. User logs in with uid/password to the account management self service portal
2. User chooses to add second factor
3. User is presented with a form to enter cardnumber (16 digits) of campus card (physical card distributed to all employees and students, card number is only available to a user by looking at the physical card) and PIN code for the card.
4. User is considered verified if the information is provided correct
5. User is allowed to add Google Authenticator
6. User is unable to remove token and can only add a new Google Authenticator by physically visiting a directory administrator and have them erase the token through the account management portal

1. FYI: The use cases we’ve identified so far:
    - InCommon Certificate Manager (Paul/Nick Roy/Comodo)
    - Federation Manager (Paul/Nick Roy)
    - WorkDay (we'll need to find someone to contact)
        - Background information
            - SAML MFA for WorkDay
            - https://community.workday.com/idea/90665 (WorkDay login required)

        - The WorkDay Working Group
            a. Mailing list: workday@incommon.org
        - Other cloud services?
    - LIGO (Scott Koranda)
        - Other VOs?
        - Scott Koranda has asked and received from InCommon a mail list targeted at InCommon Participant “Government and Nonprofit Laboratories, Research Centers, and Agencies” organizations. He will in the next few days start a thread to try and get input from those organizations. If any input is received he will summarize and bring it back to this call.
    - Federal services (FICAM)
    - Intra-campus use cases (Dave Langenberg)
    - Federated AuthN to a single Grouper instance (Keith)
        - Probably others.
2. Answering our current questions
    - See table below.
    - Which should we answer in our base-level MFA profile?
    - Which should we leave for future work?
    - How many can we answer today?
    - How will we organize the profile spec to answer these questions.

Current Questions

	Question	Base-Level MFA Requirement	Stronger Level Requirement	Base-Level with Mutual Authentication	Future Optional Spec
1	Do we want to call phishing out specifically? There are, of course, other risks, such as man-in-the-middle. - What are the risks we address? How do we state them in the spec?	Improperly disclosed (unprotected) transmitted secrets not usable (a) more than once; or (b) after an X minute window after disclosure. Threats addressed: password phishing	Protects against man-in-the middle attacks (verifies agent requesting credential is the correct agent) BS:Not as a requirement of the spec, but as a statement of the means of the authentication and the means of the registration process		
2	Do we allow "trusted" access devices (PCs, phones, etc.)?	yes	maybe -- perhaps limited to exclude netblock-trust? BS: Splitting hairs between saving a cookie for trusted, and registering a device to get SMS/Soft Token/Voice access. Both are providing something you have. So this needs to be addressed by looking at provisioning process (Q 7)		
3	How long can the SSO session be?	EG: Any the authenticating organization allows anyway.	EG: 8 hours with support for ForceAuthn for re-authning both factors (I had to say it!) BS: An AuthN Instant seems to allow the SP to decide. Better would be metadata extension or AuthN Request statement that states how long the SP will allow		
4	Do we allow "fail open?"	Yes, with appropriate signaling No! (Not without signalling!) +24 EG: for me, signalling “fail open” means saying “didn’t do second factor”, which is equivalent to “no” DL: Operational realities will require business continuity which will win every time over our desires. public/well-known location posting of fail-open periods will allow services to more carefully scrutinize actions done during the fail-open period. (+1, we have built this option into our MFA deployment for SSO) BS: Yes, if the campus fails the 1st factor open as well ;)	Definitely no.		
5	Is a second factor that is unlocked with the first factor (e.g., VOIP phone) really a second factor?	No, but how is that specified? (EG: Out of scope/advisory for base level? +1) BS: This really needs to be treated the same as question #6			

6	Can a second factor be registered solely on the basis of the first factor?	EG: Allowed with an initial registration period? DL: Allowed for initial registration open anytime / Denied for re-registration device-recovery?	EG: Allowed only with separate vetting?		
7	In general, is the registration process "strong enough?"		EG: Duplicate of #6 above?		
8	Do we want to identify technologies?	no			
9					
10					
11					
12					

- Eric: We should define what needs to be in the base level v1.0 (first column). Other things are for the future.
- For next week, please add your comments to the table, including your initials so we know who's saying what.

Work Group Call - February 11, 2016

Attendees

- David Walker, Internet2
- Karen Herrington, Virginia Tech
- David Langenberg, uchicago
- Scott Bradner, Harvard U.
- Tommy Doan, Southern Methodist University
- Nick Roy, Internet2
- Scott Cantor, tOSU
- Nick Lewis, Internet2
- David Bantz, U Alaska
- Paul Caskey, Internet2
- Eskil Swahn, SWAMID / Lund University
- Kari Robertson, UCSC
- Mary Dunker, Virginia Tech
- Russell Beall, USC
- Eric Goodman, University of California
- Mark "Max" Miller, Penn State
- Ayesha Benjamin, UCF
- Brad Schwoerer, U of Wisconsin-Whitewater

Agenda and Notes

1. Welcome
2. Agenda bash
3. Use cases
    - Who is going to use our profile? Some possibilities include the InCommon/Comodo Certificate Manager, the InCommon Federation Manager (metadata management for Site Admins), and WorkDay. Last week, we also thought there are probably research-related possibilities like CILogon. Will people use the profile for use cases that are internal to their campuses?
        - A recent note from Scott Koranda: "I want to reiterate that if the MFA profile evolves in a way that crosses national federation boundaries then it is likely to be quite useful to research VOs like LIGO."
        - Paul Caskey: Interest from feds in something stronger than "basic" identity, and Silver hasn't caught on. MFA can make that differentiation.
            - Paul can brief FICAM about what we're doing and get feedback.
        - Dave Langenberg: Chicago is using this in a campus-centric use case.
        - Nick Lewis: WorkDay and Duo are having discussions.
        - Max Miller: Is on the WorkDay group. It's not active now, but WorkDay has said that they'll be forming a higher-ed-related group.
            - Scott Cantor: WorkDay does have this on their issue list. Our work may provide an incentive to do something.
        - Eric Goodman: Discussion of whether our profile is useful if the SP doesn't really "care" about authentication strength. E.g., if SP just replaces "PasswordProtectedTransport" with "MFAAuthnContext", but doesn't operate in any other way that makes the MFA context meaningful, then the profile doesn't provide much value, as the SP will still rely on the IdP to address any "special" access rules.

        - Scott C: Even if the SPs don't do anything differently, there's still value to the IdP operator if they don't need to manually configure MFA support via per-SP configurations.
        - Agreed(?) that if an SP asserts the profile and requests MFA, the SP operators are taking on the responsibility for dealing with "failed MFA" situations. This point should probably be spelled out as guidance.
            a. "Handling failed MFA" may by simply mean refusing users access until MFA is asserted by the IdPs
            b. Could also be dealt with by SPs accepting multiple authncontexts ("prefer MFA, accept PPT").
            c. Dave L: We may want to consider other forms of signalling of "failed MFA". E.g., an IdP could post a notice of "Failed MFA during $TIME_PEROID" to a well known location for which SPs would monitor and could scrutinize activities more closely. This would enable campuses to fail-open when MFA providers fail and still assert MFA Success to enable business continuity.
    - We'll want to talk to these people to answers questions about what needs to be in or out of our base-level MFA profile.
4. Continued discussion of Paul Caskey's language for the base-level MFA profile.
    - "When SAML Authentication Context 'xyz' is used in a SAML Authentication Request or subsequent SAML Authentication Response, the meaning of that value is that a discrete second factor will always be (or was) used in the initial authentication event for the current web SSO session. Such second factor will be resistant to phishing attempts and will be used regardless of the user's device or location. Normal SSO session options (duration, etc) are allowed."
    - Things we discussed last week:
        - We may not want to call phishing out specifically. There are, of course, other risks, such as man-in-the-middle.
        - Do we allow "trusted" devices?
        - How long can the SSO session be?
    - What questions about this language should we ask of the people responsible for our use cases?
        - Should the profile allow "fail open?"
        - Eric: "Phishing" issue; the (at some point) proposed wording of "not likely to be phished at the same time the password is phished fails the "man-in-the-middle" attack. We talked broadly about "reusable phishable information" last week.
            - This led to discussion of whether "recovery code" type solutions (written down one-use passcodes, HOTPs, etc) would fail the "reusable" test, if the stored code is reusable multiple times.
        - Scott C. raised the question of whether we are intending to signal literally "MFA" vs. "strong authentication". "MFA" by itself seems to rule out certificate authentication
            - Mary: Certificate can itself be protected by password/pin. Scott was comfortable that this would bridge his concern.
            - Some (quick) discussion of whether password/pin protection of the external "strong" token should be considered MFA. (Eric's inserted interpretation:) The question being whether both factors need to be authenticated directly by the IdP, vs. processes that require MFA by policy/practice.
                a. I.e., with Duo, the IdP typically authenticates both the PPT and the Duo authentication success. With pwd-protected cert, the IdP presumes presentation of the cert-based authentication implies both factors were used.
        - Should we consider registration process in whether this is MFA? What if second factors can be registered knowing only the first factor?
            - David W: Suggestion that this trustmark/authncontext/profile strictly indicate that MFA (or otherwise acceptable "strong" encryption") technology/process was done. While registration processes are important and relevant, those can be defined separately and combined with this profile once they are finalized.
            - Signalling for non-authentication "trustmarks" can be done through channels other than authnContext.
            - Other trustmarks will be needed. We can suggest some of those as part of our work.
        - (Didn't get the name) Discussion of whether telephony based MFA is really strong encryption. Argument that strong encryption would require strong registration practices, and protections beyond what would be available on a typical (non-keycode protected) phone.
            - Nick: campuses aren't going to be able to meet that high a level of "assurance"; could run into the same adoption issues as Silver. And even then, OMB 05-05/NIST 800-63 define levels above 2 that those examples may fit.
            - Paul: probably need to distinguish initial registration from "re-registration" in any such profiles (and possibly disallow methods that permit 'at-any-time' re-registration).
                a. Though these registration profiles may still be different profiles than the MFA profile this group builds first.
        - Eric's VOIP example: What if the phone is the second factor, but the first factor is used to authenticate to the phone?
            - Is this really a second factor? Everyone pretty much agrees "no". However, it may be a challenge to distinguish what makes this authentication process insecure, yet still NOT address registration security.
    - Quick FYI: Duo Security Outage - Responses and Planning for Future was created to collect mitigations for Duo's recent outage at various campuses.

==========

Work Group Call - February 4, 2016

Attendees

Karen Herrington, David Walker, Emily EIsbruch, Scott Bradner, Scott Koranda, Bradley Schwoerer (U of Wisc-Whitewater), Mark McCoy (UTSA), Roger Safian (Northwestern), Nick Roy (I2), Sean Sweeney (PITT), Jim Jokl (Virginia), Nick Lewis (Internet2), Eric Goodman (University of California), Tommy Doan (Southern Methodist University), Eskil Swahn (SWAMID, Lund University), Stefan Metzger (DFN), Mike Grady (Unicon),Theresa Semmens (NDSU), Brendan Bellina (UCLA), Helen Fankhauser (U of NE), Rob Pierce (Sewanee), Ayesha Benjamin (UCF), Mary Dunker (VA Tech), Russell Beall (USC), Keith Hazelton (UW-Madison)

Agenda and Notes

Welcome

Introductions

Background

This working group is chartered by the AAC, InCommon Assurance Advisory Committee.

Previously Jacob Farmer, Indiana University led this working group in 2015.

There were two subgroups

Previous Subgroups for the MFA Working Group

- Use Cases Subgroup
- Technology Subgroup?

Link to Charter for this Working Group

scope - need to have common understanding of limited scope for 1st phase of work

David Walker: Much interest in the output of this WG

- There is relation between the output of this working group and the Cert Service manager.
- The work of this group can also come under the TIER first release in April 2016.
- There is interest from IDESG (Identity Ecosystem Steering Group) and Kantara

There is urgency to deliver.

We should deliver a really simple MFA profile for phase 1 (in early April). An “MFA was Done” profile.

Then we could modify the charter to continue to more complex issues.

Eric, UCOP: that makes sense. Focus on “what’s the signaling.”

Need to be able to indicate “Failed (MFA only)” or “Unable to comply” to the SP or IDP.

May be a functional requirement of SP or IdP that they be able to send (or consume and rationally reply to) such messages in order to claim “compliance” with profile. E.g., an SP that requests MFA MUST also accept Password; even if response is just “sorry you need MFA” when Password is provided (This is an example, not a specific proposal)

David: Limit the scope for now to SAML Authentication Context signaling

Nick Lewis - agree with David’s point about simple and leave complex issues out (that might be service provider specific like Duo)

Mike Grady: may want understanding of “remember me”

Karen: getting to that level can be complex

Scott K: Expressed desire for a single approach across SAML higher ed identity federations, for example eduGAIN (not just InCommon-focused)

Eskil: I'm here at least. SWAMID (Sweden). We are currently starting to roll out MFA in our federation. We are interested of course to end up with a similar profile to yours/ours

David: Here's Paul Caskey's language that I just mentioned: "When SAML Authentication Context 'xyz' is used in a SAML Authentication Request or subsequent SAML Authentication Response, the meaning of that value is that a discrete second factor will always be (or was) used in the initial authentication event for the current web SSO session. Such second factor will be resistant to phishing attempts and will be used regardless of the user's device or location. Normal SSO session options (duration, etc) are allowed."

- OTP is time-dependent resistant to phishing, but not man-in-the-middle.
- David: Perhaps we should just say that the second factor is unlikely to be compromised when the first factor is compromised, not that it's resistant to phishing.
    - In parsing this statement we still had concerns (actual phishing likely to get both at the same time)
- Issue may be whether the second factor is "statically reusable" (storable for use later)?
- We'll continue this discussion next week.

Outcomes of today's call

- Start with simple, vanilla MFA profile, then enhance.
- We'll continue to work on Paul's language.
- David will send calendar invitation with links to notes, etc.

Questions we'll have to answer…

- Was MFA verified just now, or
    - is there an SSO session?
    - Is this a trusted network location?
    - Is this a trusted access device? ("remember me")
- Is goal anti-phishing vs. "higher assurance"? (related to whether "remember me" is "acceptable")
    - General consensus is "anti-phishing" (or whatever descriptor we come up with). This could be a component of "higher assurance", but the focus is on improving reliability of the authentication event overall.
- Are we looking at a single profile, or multiple levels?
- Need to understand what service providers want.
    - ScottK: Most SPs he's talked to focus more on credential strength than attribute vetting when asking for "higher LoA".
- Are we looking for a self-asserted attribute or an attribute that can only be asserted after a formal review process has been completed?

timeline

deliverables

Action Item Summary

Next Call: Thursday, Feb. 11 at 4pm ET

==========

Use Cases Subgroup Agenda - September 8, 2015

- Roll Call (if you are viewing the Google Doc, feel free to add yourself)

    - Eastern Time Zone
        - Scott Bradner (Harvard)
        - Scott Cantor (OSU, Shibboleth Consortium)
        - Jacob Farmer (IU)
        - Karen Herrington (VT)
    - Central Time Zone
        - Bradley Schwoerer (U of Wisconsin-Whitewater)
        - Barry Ribbeck (Rice)
    - Mountain Time Zone
    - Pacific Time Zone
        - Eric Goodman (University of California)
    - Other Time Zones
        - Eskil Swahn (SWAMID, CEST)
- Agenda Bash
- Resume discussing IdP scenarios
    - IdP should signal if MFA happened (at least if the SP can process an “MFA happened” message).
        - See “Distinguishing characteristics of use cases (SP-signalling oriented)” (last week) for what we may want to have signalled and how.
    - IdP should signal if MFA is supported (or perhaps if MFA profile is supported) (in Metadata, likely)
        - Should lost token/MFA method be signalled?
            - No, trust is trust. If the recovery is “good enough” to call it MFA, then it’s still MFA and not a special use case.

Other things we might want to signal (at least conceptually, but perhaps not really…)

- MFA “LoA” separate from the password “LoA”
- Specific MFA technologies
    - Thinking is that at least at start there’s only one category: “Approved somehow”.
    - That is, the profile would list excluded mechanisms, and those not excluded would be allowed.
        - Probably require that deployers implicitly assert that what they are using is “as good” as the “non-excluded” ones?
        - Issue is that if you white list specific technologies, then you can never release a new one (without forcing all SPs to update their accepted lists)
    - Or (I misunderstood the original comment) the signaling would name specific technologies to exclude, or the IdP would signal what specific technology was used and the SP would be at liberty to reject.
        - Would require a categorization of technologies
            - is Duo the same as MS “Phone Factor”, or a different one)?
            - is Duo SMS/call the same as Duo push?
            - I would be careful about trying to categorize technology if you really mean to try to differentiate strength of authN (EG: Don’t disagree, was calling out the questions that flowed from the req’t statement about disallowing specific technologies, at least for me)
    - Ultimately the profile needs to be able to evolve with the technology.
    - Isn’t one way rather to have two or three categories of MFA technologies (say low, mid, high) and try to list requirements to qualify for the different categories? I can’t really see how we keep track of all technologies available.. (EG: ibid last comment…)
- Should the SP have a standard way to signal what resource is being accessed? E.g., URL or function being accessed.
    - There’s an argument that if there’s anything to re-initiate an AuthN, that thing (Proxy, WAF, whatever) could have the intelligence to inject the MFA signal.
    - This would support the use case where the SP knows that a given resource is “special”, but doesn’t know who needs MFA to access it.
- ForceAuthn
    - What does it mean, esp when MFA is a separate factor (two step MFA vs. one step MFA)?
        - Would the general process kill the existing SSO session and thus imply that forceAuthn will always end up re-authenticating both factors?
            - Yes, but there are cases “in the wild” where deployers are separating the factors such that you can reauth just one of them.
    - How to balance an app’s desire for MFA with the cost of reauth.
- Is MFA per SP, or per IdP session?
    - And what does authninstant mean for MFA?
- IdP forces MFA independent of inband SP signalling << These might be nice features that a product could support, but are out of scope from an “interop profile” PoV.
    - IdP force MFA for specific SPs (presumably as the result of an out of band negotiation/requirement) Geographic location triggering this?
    - IdP force MFA for specific users
        - end user opt-in
        - Common circumstance is users with admin rights in some applications being required to use MFA everywhere (by policy at IdP, for simplicity)
    - IdP force MFA for capricious reasons
    - (May not require signalling)
    - Is there a concept of IdP signalling “I did MFA if it was required for this user”
        - I.e., SP knows that MFA might be required but not who needs it (deferred to IdP)
        - Sounds like the answer is “no”. Why the IdP did MFA is out of scope.

==========

Use Cases Subgroup Agenda - September 1, 2015

- Roll Call (if you are viewing the Google Doc, feel free to add yourself)
  - Eastern Time Zone
    - Scott Cantor (OSU, Shibboleth Consortium)
    - Jacob Farmer (Indiana)
    - Scott Bradner (Harvard University)
    - Karen Herrington (Virginia Tech)
    - Aaron Wilkey (University of Notre Dame)
  - Central Time Zone
    - Bradley Schwoerer (U of Wisconsin-Whitewater)
    - Peseng Yu (Rice University)
    - Barry Ribbeck (Rice University)
    - Brett Bieber (U of Nebraska-Lincoln)
    - Keith Hazelton (UW-Madison)

    Mountain Time Zone

  - Pacific Time Zone
    - Eric Goodman (University of California)
    - Russell Beall (University of Southern California)
  - Other Time Zones
    - Eskil Swahn (SWAMID, CEST)
    - Stefan Metzger (DFN Germany, CEST)
- Agenda Bash
- Resume discussion about generic use cases
- Turn them into something better structured for external consumption
  - Core generalized scenarios
    - IdP forces MFA independent of inband SP signalling
      - IdP force MFA for specific SPs (presumably as the result of an out of band negotiation/requirement) Geographic location triggering this?
      - IdP force MFA for specific users
        - end user opt-in
      - IdP force MFA for capricious reasons
      - (May not require signalling)
    - SP requested MFA (signaled via some interop profile)
      - SP require MFA for all users
      - SP require MFA for specific users
        - end user opt-in
        - users that meet a certain criteria which may be expressed in terms of user identity or meeting a more generalized criterion
        - Persistence would be nice
        - How to address/avoid multi-step authentication process (user does login non-MFA then SP looks user up and forces user to re-login using MFA)?
      - SP require MFA for specific transactions (e.g., escalation)
        - Persistence may not be relevant
      - SP request MFA non exclusively, meaning it would only allow non-MFA users access to “non-sensitive” functionality
      - SP request no MFA to constrain costs; consider IdP as a service where there is a cost per AuthN
      - SP requests forceAuthn (is this in scope?)
        - Does this mean re-auth pwd, 2nd factor or both?

- possible reference points for use case documentation (KeithH)
  - http://alistair.cockburn.us/Basic+use+case+template
  - http://alistair.cockburn.us/Resources+for+writing+use+cases
  - just for fun: http://alistair.cockburn.us/oath+of+non-allegiance

- Name
- Description
- Pre-reqs
  - SP
  - IdP
  - Metadata
- Advantages
- Disadvantages

UC SP-01

Description: SP require MFA for all users. Typical situation includes a SP handling sensitive research information with requirements for IT/IS-security.

Pre-reqs

- SP signal authnContext to IdP

Advantages: The SP is in complete control of the business logic.

Disadvantages: No fallback for users lacking MFA capability.

Distinguishing characteristics of use cases (SP-signalling oriented):

- Metadata can indicate all users will require MFA
- Metadata (or assertion) can indicate not all users require MFA but non-MFA supported
- Metadata (or assertion) can indicate that users will lose access rights if non-MFA, but non-MFA accepted
- Assertion can indicate MFA required in this instance (no extra info)
- Assertion can indicate this specific user will always require MFA (“I will always ask for MFA for this user”; presumes two-step at least once)
- Assertion can indicate a business rule for requiring MFA (“all ePA=Faculty require MFA”)
- Assertion can indicate choice of MFA or no-MFA

Use Cases Subgroup Agenda - August 25, 2015

- Roll Call (if you are viewing the Google Doc, feel free to add yourself)
    - Eastern Time Zone
        - Jacob Farmer (Indiana University)
        - Scott Cantor (OSU, Shibboleth Consortium)
        - Scott Bradner (Harvard U.)
        - Aaron Wilkey (University of Notre Dame)
    - Central Time Zone
        - Peseng Yu (Rice University)
        - Roger Safian (Northwestern University)
        - Bradley Schwoerer (University of Wisc-Whitewater)
    - Mountain Time Zone
    - Pacific Time Zone
        - Eric Goodman (University of California)
        - David Walker (InCommon)
    - Other Time Zones
        - Eskil Swahn (SWAMID, CEST)
        - Stefan Metzger (DFN Germany, CEST)
- Agenda Bash
- Welcome
- Open discussion on how to compile use cases
    - Core generalized scenarios
        - end user opt-in
        - IdP forces MFA independent of inband SP signalling
            - IdP force MFA for specific SPs (presumably as the result of an out of band negotiation/requirement) Geographic location triggering this?
            - IdP force MFA for specific users
            - IdP force MFA for capricious reasons
            - (May not require signalling)
        - SP requested MFA (signaled via some interop profile)
            - SP require MFA for all users
            - SP require MFA for specific users
            - SP require MFA for specific transactions (e.g., escalation)
            - SP request MFA non exclusively, meaning it would only allow non-MFA users access to “non-sensitive” functionality
            - SP request no MFA to constrain costs; consider IdP as a service where there is a cost per AuthN
    - Other considerations
        - Communicate type of MFA (is that necessary)?
            - Are there minimum requirements/characteristics of a second factor?
                - E.g., is a second password or a PIN a second factor per this profile? (Hopefully not!)
            - We have talked loosely about “high” and “low” MFA and can see a situation where this could be useful (two AuthContext for example)
        - Password and Second factor are authenticated at different time
            - Do we care?
            - What’s the authnInstant that should be captured in the authnresponse?
            - If forceAuthn is requested by the SP, do both factors need to be re-tested?
        - Metadata represents the IdP’s ability to support MFA or SP’s expectation for support of MFA?
            - For some users?
            - For all users?
        - Should Federation certify IdP’s implementation?

        - Do we need error codes or error messages for “MFA not available” for the specific user? (Not sure the use case…) (perhaps “SHOULD provide useful user messages” type language)
            - At IdP level
            - At user level
            - Does user get redirected to SP with error message, or do they stop at IdP (as failed login) vs. return a SAML error code to the SP
            - Is this just out of scope?
            - Profile should have ability for IdP to signal failure to SP. Whether that signalling is used is up to the IdP.
    - Format/template of use case documentation for submission/feedback?
        - Google form?
    - Quick documentation of two identified use cases from SWAMID:
        - SPs with high security needs where the SP would like encapsulate the entire login session behind MFA authentication. An example here would be a login handler to Shibboleth available to SPs by the use of a specified AuthContext. Rather transparent to the SPs which need only to request the specific AuthContext. (SP requested MFA for all users)
        - SPs with high security needs for specific functionality. An example here would be an SP which use normal user credentials (ePPN/password for example) to allow initial access to the SP and then need to verify the user with a higher certainty when the users uses certain functionality. To clarify, you could for example have an SP which allow users to browse invoices by logging in with normal credentials but the SP would have application based functionality to verify a MFA based credential (through for example a web service) if the users actually want to sign off one of the invoices. Also fairly easy to implement technically but with the drawback that you need specific application based logic to handle every case. Perhaps not an issue in self-developed web applications but a bit tougher to expect normal vendors to implement. (SP requested MFA for specific transactions)
        - Our internal discussions so far have been that the best way to implement this would be as a technical profile that supplements the SWAMID Assurance Level 2 (identified individuals) and we have so far not seen any use cases by us where it would be interesting to use this profile as a supplement to SWAMID Assurance Level 1 (unidentified individuals).
    - (Barry) - While I could not make the call due to conflicting schedules, I would like to caution on the use of escalation of privs as a use case. My understanding is that since we can not be assured of the LOA of the 2nd factor, that a 2nd factor should not be assumed to provide better security

Archived notes from full group meeting on 8/5/15

Agenda - August 5, 2015

- Roll Call (if you are viewing the Google Doc, feel free to add yourself -- good idea, Eric!)
    - Eastern Time Zone
        - Scott Bradner (Harvard)
        - Max Miller (Penn State)
        - Mary Dunker (Virginia Tech)
        - Rob Stanfield (Purdue)
        - Karen Herrington (Virginia Tech)
        - Steve Carmody (Brown)
        - Jacob Farmer (IU/AAC)
        - Scott Cantor (OSU)
    - Central Time Zone
        - David Langenberg (University of Chicago)
        - Brett Bieber (Nebraska-Lincoln)
        - Keith Hazelton (UW-Madison)
        - Tom Jordan (UW-Madison)
        - Charlie Calderon (UW-Madison)
        - Bradley Schwoerer (UW-Whitewater)
        - Paul Caskey (Internet2 T&I, Austin)
        - Barry Ribbeck (Rice University)
        - Paul Engle (Rice University
        - Peseng Yu (Rice University)
        - Roger Safian (Northwestern University)
        - Theresa Semmens (North Dakota State University)
        - Mike Grady (Unicon)
    - Mountain Time Zone
        - Nick Roy (Internet2 T&I, Denver)
        - Ann West (Internet2 Trust and Identity - Denver)
    - Pacific Time Zone
        - Dedra Chamberlin (Cirrus Identity)
        - Eric Goodman (UC Office of the President)
        - David Walker (Internet2 T&I, MFA Cohortium)
        - Russell Beall (USC)
    - Other Time Zones
        - Stefan Metzger (DFN Germany, CEST)
        - David Bantz (U Alaska)
        - Laas Toom (HITSA, Estonia, EEST)
        - Eskil Swahn (SWAMID, Lund University, Sweden, CEST)
- Agenda Bash
- Welcome
- Overview of Charter, Goals, and Timeline
    - Clarify what interop means in this context

        - consistent way to require MFA in the context of a service
        - About an SP being able to rely on a standard syntax/semantics when making the request of any IdP
    - Standard Authentication Contexts
    - More clearly call out that we're discussing a SAML profile if that's what we really mean
    - Provide some clarification regarding what "current technology" means -- Duo vs RSA and/or SAML
    - Deliverable 2: Clarify that "widely deployed" means in the HiEd vertical. Technologies that IdPs have in production.
- Discuss proposed sub-groups and parallel efforts
    - 1 & 2 in parallel
    - 3 & 4 in parallel
    - Draft materials sent to the whole group
    - Clarify participation in large group does not require participation in subgroups
- Overview of survey -- https://docs.google.com/document/d/15ccv_GgWd52Xw6db8PpxrYt0nrdcl0ygK8SIcuIgI34/edit?usp=sharing
- Open discussion
    - www.lightbluetouchpaper.org/wp-content/uploads/2012/05/matrix.png from http://research-srv.microsoft.com/pubs/161585/QuestToReplacePasswords.pdf
    - http://arxiv.org/pdf/1309.5344.pdf
        - Consider also accessibility
    - Cohortium resources
        - How Much Security Is Enough?
        - Multi-Factor Authentication Solution Evaluation Criteria

Blank Template for Reuse

Group Type Agenda - Date

- Roll Call (if you are viewing the Google Doc, feel free to add yourself)
    - Eastern Time Zone
    - Central Time Zone
    - Mountain Time Zone
    - Pacific Time Zone
    - Other Time Zones
- Agenda Bash
- Welcome