Draft FIPS 201-3 Virtual Public Workshop, Q&A Transcript-

Event date: Wednesday, December 9, 2020, 8:30 a.m. – 1:00 p.m.

Below is the transcript of the Q&A chat from Draft FIPS 201-3 Virtual Public Workshop. Q&A are provided. It is provided uncut – except that event logistics questions were removed (e.g., questions on audio/video issues or on conference proceedings).

Comments received via Q&A are not considered official comments for Draft FIPS 201.3. To formally submit comments please follow commenting process outlined in Request for Comments on Federal Information Processing Standard (FIPS) 201-3.

The video recording from the workshop presentation is available here.

Additionally a copy of the presentation slide deck is available here.

[09:16 AM]
Michele Cohen asked : Do you view FIPS 201-3 a key management system? Does it follow the NIST guidance for a key management system SP 800-57 part 1 rev 5?
1 upvote | 1 answer | 0 reply

Andy Regenscheid (NIST) answered -
The PKI that provides the foundation for PIV credentials can be viewed as a particular type of key management system. Our specific requirements and guidelines in FIPS 201 and the associated Special Publications are informed by and aligned with the broader cryptography and key management guidelines that are also developed by NIST.

[09:19 AM]
Martin Baltiyski asked : In the context of "Zone 2B - Issuer Identification Number", what are the definitions of "department code" and "agency code"? In all other places in the document, department and agency are used interchangeably, but this is the only place where they are considered separately.
0 upvote | 1 answer | 0 reply

Jonathan Gloster answered -
We will address this in a later presentation

[09:20 AM]
Martin Baltiyski asked : Where are the department codes and agency codes defined for use for the Issuer Identification Number? Can you give an example of an Issuer Identification Number and where you got the values for department code and agency code?

5 upvotes | 0 answer | 0 reply

[09:31 AM]
Bill Windsor asked : Q for J. Burris - Will OMB play a more proactive role in how federal agencies will be held accountable for employing appropriate solutions for issuance and access control needs?
2 upvotes | 1 answer | 1 reply

Jordan Burris answered -
Hi Bill - OMB's role will be consistent in proactively engaging with Agency leadership regarding our expectations for identity management. This will continue to be managed through the budget process, Metrics, and engagement through the President's Management Agenda / President's Management Council.

Bill Windsor replied -
Thank you Jordan - i recognize some agencies are struggling to make access control a priority.

[09:34 AM]
Michael Lawlor asked : Will guidance be provided around the requirements for physical presence to verify identity? for example couldn't fingerprints and photo's (normally captured at GSA facilities) be done live via a mobile phone?
3 upvotes | 1 answer | 0 reply

Jonathan Gloster answered -
We will have a discussion on remote supervised identity proofing in a later presentation

[09:34 AM]
Stephen Howard asked : How long can we expect the OPM pandemic guidance around fingerprints to be in effect? Eventually, we will need to finish a screening/vetting using fingerprints. When might this be required again?
2 upvotes | 1 answer | 0 reply

Dorianna Rice answered -
The guidance is still in effect and we continue monitoring agencies to see how they are able to obtain prints.

[09:36 AM]
Stephen Howard asked : Investigating use of mobile device cameras to capture fingerprints, it seems VERY feasible. Yet we run into the conflict with FBI EBTS for CHRC and related checks. Is OPM working with FBI to update EBTS to accommodate mobile device cameras for imaging fingerprints?
2 upvotes | 1 answer | 0 reply

Greg Fiumara answered -
NIST has been exploring the use of mobile device cameras for fingerprint capture. Please refer to NIST IR 8307 for the latest details on their use and performance: https://doi.org/10.6028/NIST.IR.8307

[09:42 AM]
Bill Windsor asked : Maybe it will be covered later, but I will ask now - will SP800-116 come under review as a result of FIPS 201-3 and SP800-63 updates?
2 upvotes | 3 answers | 3 replies

Hildy Ferraiolo answered -
Hi Bill, Yes, it will be updated. SP 800-63 is not an exact match for assurance levels for PACS ... more in the 10:25 am session

Jonathan Gloster answered -
We will address documents to be updated based on FIPS201-3 in s later presentations

Bill Windsor replied -
Thanks Hildy - i agree alignment is not an exact match - but maybe through future discussions we may be able to close some of the gaps.

Jim Fenton answered -
Note that physical access is out of scope for SP 800-63, so 800-116 is somewhat independent in that respect.

Bill Windsor replied -
Agreed Jim, however, I believe we should strive to associate IAL and AAL factors to operate hand in hand with physical access control?

Bill Windsor replied -
A documented correlation of facility risk / vulnerability needs to cross walked with AAL per 800-63. ISC should be engaged for the discussion.

[09:43 AM]
Hussain Jafri asked : Andy keeps cutting in and out
3 upvotes | 1 answer | 0 reply

Jonathan Gloster answered -
we are aware . thanks

[09:46 AM]
Cynetheia Brown (DOS) asked : Is there a way to translate LOA to xALs.
This would be especially useful for authoritative documents that have not updated assurance level language i.e. 800-157

1 upvote | 2 answers | 0 reply

Jim Fenton answered -
Since the detailed requirements for the xALs don't confirm exactly to the requirements for LOAs used previously, there isn't an exact correspondence.

Jonathan Gloster answered -
will be addressed in 10:00 session

[09:47 AM]
Camey Trossbach asked : We need to have further discussions about CHUID authentication. May the CHUID continue to persist on the card regardless of it being a deprecated auth mechanism?

1 upvote | 2 answers | 1 reply

Justin Richer answered -
Yes, the CHUID element is not being deprecated but the authentication mechanism is removed. See the note here: https://pages.nist.gov/FIPS201/frontend/#fn:support

Camey Trossbach replied -
Thanks Justin

Hildy Ferraiolo answered -
Yes, the data object called CHUID will remain on the card to provide lookup index # for AC but cannot be used for authentication.

[09:48 AM]
Jim Thomson, MITRE asked : Maybe "PIV Account" should just be called "PIV Identity Account" as Andy [re]labeled it to avoid forever confusion with login accounts.
6 upvotes | 0 answer | 0 reply

[09:49 AM]
Steve asked : Will there be a new SP800-79 forthcoming as a result of 201-3? If so, when is that expected?

0 upvote | 2 answers | 1 reply

Hildy Ferraiolo answered -
Short answer, Yes.

Hildy Ferraiolo answered -
more details on “when” is covered in the 12:00 pm session.

Steve replied -
Will a draft be out anytime soon? Oh I see. Ok thanks.

[09:51 AM]
Michele Cohen asked : Using mobile device cameras to capture fingerprints? Most IOT has very limited or non-existent privacy and security controls at this time. That means the chain of custody for this data is not encrypted and could be intercepted. This is reason why recent bill was passed. H.R.1668 - IoT Cybersecur
2 upvotes | 1 answer | 2 replies

Jim Fenton answered -
Yes -- stay tuned for discussion on supervised remote identity proofing. For authentication, verifying biometrics on the user device is preferred, but can be done centrallly if specific security and privacy controls are followed.

Michele Cohen replied -
As the biometrics get farther from the source of truth, they loose trust. Hence need for local validation and verification.

Michele Cohen replied -
Its not just the data regarding individual that has to be assessed. Its the equipment and processes that are used to protect the data and chain of custody.

[09:52 AM]
Timothy Schmoyer asked : Is there a difference between Identity Federation and identifiers versus Authentication Federation and authenticators? Does a credential binding identity and authenticator provide both identifier and authenticator for federation?
0 upvote | 2 answers | 1 reply

Justin Richer answered -
Yes, there is a difference, and we will cover those difference in detail at the 11:30 am session.

Justin Richer answered -
Also we will cover the differences in identifiers as well -- short preview is that they are

separate layers that build on each other.

Timothy Schmoyer replied -
Thank you! :-)

[09:55 AM]
robert schlecht asked : The Federation SAML does not specifically specify PIV Authentication at your CSP. How to do guarantee PIV-Auth was used at the CSP? Or, is there an SAML default Attribute that can convey PIV-Auth?
1 upvote | 0 answer | 0 reply

[09:56 AM]
Mark Russell asked : Will NIST provide guidance on how to convey IAL and AAL in assertions? SAML and OIDC have claims that could be used, but it would be good to standardize the specific format of this data
5 upvotes | 1 answer | 1 reply

Justin Richer answered -
The specific mechnaisms for a given protocol would be subject to a protocol-specific profile, which would not be in the form of a FIPS or SP. However, protocol-agnostic methods for conveying these values as attributes of the authentication event is something that might be a part of larger federation guidelines, which we're investigatng now (a bit more on that work at 11:30). Technologies such as Vectors of Trust (RFC8485) are helpful for communicating these things, and these values can be bound into a protocol like SAML and OIDC.

Mark Russell replied -
makes sense... thanks!

[09:56 AM]
Michael Lawlor asked : Will the use of newer capabilities such as block chaining for identity be considered during these discussions?
3 upvotes | 1 answer | 0 reply

Andy Regenscheid (NIST) answered -
We will discuss how FIPS 201-3 will accomodate new and emerging authenticators in the Derived PIV Credential session after the break.

[09:56 AM]
Dave Wilson asked : With regard to CHUID: I believe there is at least one interagency authenticator related to use of legacy equipment (Mainframe) that offers pseudo PIV authentication via CHUID? Is there some formal process we should be using to bring this to

somebody's attention?

0 upvote | 1 answer | 2 replies

Hildy Ferraiolo answered -
Could you leave a public comment for this, please?

Dave Wilson replied -
Hildy, I think this is the program you spoke with me about in which I expressed concern about the middleware being proposed? My assumption is this was authenticating via CHUID, but please let me know if I'm off base in my technical understanding.

Dave Wilson replied -
I am clearly incorrect based on your presentation, which informed me that CHUID is a wireless authenticator. Thanks.

[09:58 AM]
Kenneth Myers asked : Under what conditions is PIV logical authentication AAL3?
0 upvote | 2 answers | 1 reply

Hildy Ferraiolo answered -
Using PIV PKI and PIN, for example (PKI-Auth) authentication mechanism with PIV Card.

Kenneth Myers replied -
A PIV issued from a moderate or High security baseline system is required at AAL3?

Jim Fenton answered -
PIV issuance has more to do with IAL than AAL. AAL deals with the confidence we have that the same person is authenticating each time, so is dependent primarily on using an appropriately secure authentication mechanism.

[10:08 AM]
Judith Spencer asked : Since SP 800-63-3 is also undergoing review/revision, will needs identified by the FIPS 201-3 revision inform that activity as well?
1 upvote | 2 answers | 0 reply

Justin Richer answered -
Yes, and several members of the FIPS201 team are also directly involved in the SP 800-63-4 effort.

David Temoshok answered -
NIST intends to align revisions to SP 800-63 and FIPS 201 to the extent practicable. The

general timelines for the 2 revisions also align.

[10:08 AM]
Andrew Atyeo asked : The binding of multi session bio enrolment using bio match - the bio match isnt just fingerprints? for example a applicant that does not have viable prints - the operator can perform a facial bio check - by comparing the captured bio photo with the applicant?
0 upvote | 2 answers | 0 reply

Hildy Ferraiolo answered -
That is correct - automated mechanism must be attempted first (e.g., BIO/BIO-A authentication mechanism with iris, or face recognition).

David Temoshok answered -
Biometric comparison and verification for multiple enrollment sessions may use any biometric characteristic collected and recorded from previous sessions.

[10:11 AM]
Ross Foard (CISA) asked : Won't conflating background investigating with IAL make it hard to be able to interoperate with other organizations that are not Federal organizations?
2 upvotes | 1 answer | 1 reply

Jim Fenton answered -
We aren't creating a dependency on the entire background investigation, just that the process has been initiated. I don't understand the interoperability concern.

Ross Foard (CISA) replied -
The evidencing of all other IDPs asserting IAL will be different than the evidencing on the Federal Government. That seems odd since the Federal Government created the evidencing requirements.

[10:11 AM]
Vikki Payne asked : REAL-ID compliant - will there be exceptions for states that are still not issuing REAL-ID compliant IDs? Oregon it is 'optional' and they just started issuing in June 2020.
0 upvote | 0 answer | 0 reply

[Answered during QA session]

[10:14 AM]
Michael Lawlor asked : Can't the KIOSK be virtual?
0 upvote | 1 answer | 3 replies

Jim Fenton answered -
What would a virtual kiosk look like?

Michael Lawlor replied -
a multi-faceted application using various factors to establish and validate end points. ie.. what benefits does an in person provide vs how do we replicate those benefits digitally.

Michael Lawlor replied -
physical requirements restrict agencies abilities to require things like PIV cards for access in remote locations such as overseas environments where access to certified validators is limited.

Michael Lawlor replied -
a clarification - an app would be more like remote access to a KIOSK then the actual KIOSK itself.

[10:15 AM]
Yves Massard asked : Why supervised remote identity proofing focuses on a kiosk? For example, an applicant could be sent at home a mobile device, mobile camera and mobile fingerprint scanner, perform the supervised remote enrollment and send back the devices to the PIV issuer.
4 upvotes | 2 answers | 2 replies

Jim Fenton answered -
We need to ensure the end-to-end integrity of the process. Using devices that are not issuer-controlled introduces concerns about opportunities for impostors to fraudulently complete the proofing process.

Yves Massard replied -
those devices could be issuer controlled; for example, the mobile device could be enrolled in the PIV issuer MDM providing control on the mobile device.

Jim Fenton answered -
Certainly a reasonable comment to make. The types of sensors, overview camera, etc. we expect to be used aren't typically accommodated on mobile devices, at least currently.

Yves Massard replied -
actually, you can today procure on the market today an overview camera that works with a mobile device as well as FBI certified fingerprint reader, providing the ability to create a mobile enrollment kit compatible with supervised remote enrollment requirements from SP800-63.
This enables a very lightweight mobile enrollment kit that can be shipped to applicants

while still being compliant with 800-63 supervised remote enrollment.

[10:15 AM]
Stoicho GIzdov (LS3) asked : Is the intent of the "Enrollment record" lifecycle to be a 1:1 with a "PIV Account" (as the term was defined earlier) within an agency or even across multiple agencies/departments (in accordance with NIST SP800-156)? Are there controls suggested to link/reference cross agency Enrollment records?
2 upvotes | 2 answers | 0 reply

Andy Regenscheid (NIST) answered -
Enrollment records refers to the collection of records maintained by the PIV issuer from teh registration/issuance process. While FIPS 201-3 leaves many details on what particular records are required to be maintained, we generally expect most, if not all, PIV issuers will maintain an archive of records from the registration process. FIPS 201-2 previously included the concept of the Chain-of-Trust records, was a data format for passing enrollment information to another agency (e.g., if, for instance, an employee transfers to a different agency). Enrollment records are a generalization of the type of data that could have been included in the Chain-of-Trust.

Andy Regenscheid (NIST) answered -
There are some high-level requirements and recommendations in the draft FIPS 201-3. Additional requirements may be specified in the forthcoming update to SP 800-79.

[10:18 AM]
Glen Lee (LANL) asked : many remote locations of users are in states where agency doesn't have a facility. how does FIPS remote in-person proofing and enrollment support this use case in times of COVID where users cant cross state lines without 14-day quarantine?

7 upvotes | 2 answers | 2 replies

Jim Fenton answered -
We sincerely hope that COVID-19 will be a thing of the past by the time this revision is completed, so hopefully we don't need to focus too much on the specific pandemic restrictions. However, hopefully agencies will share supervised remote identity proofing facilities as they share enrollment facilities now.

Glen Lee (LANL) replied -
It really isn't obvious how remote-in person identity proofing and enrollment is different than what we are doing today. If we require a user to go to a facility, then may as well go to a facility that is full-service.

Jim Fenton answered -
One difference (and my use of the term "kiosk" I now realize doesn't covey this) is that the equipment can be transported from place to place and that this can be done more economically than current in-person processes.

Glen Lee (LANL) replied -
GSA USAccess has offered mobile credentialing units for many years without the new requirements in FIPS 201-3 Draft. The requirement for there to be a manned operator present of controlled equipment for remote in-person is no different than what we are doing today. I'm to understand if there is any benefit of the new requirements in 201-3 for our agency.

[10:18 AM]
Debbie asked : As persons identity is finite, however, the employment cycles and varying, disconnected ICAM issuing systems are not. Why not centralize the enrollment service, collecting biometrics and interface with investigative services, by establish one authoritative source?

4 upvotes | 0 answer | 0 reply

[10:20 AM]
Debbie asked : Furthermore, issuing agencies could then interface with this authoritative to obtain a payload containing specific data needed to create and personalize the PIV card or other credential for the specific agency.
0 upvote | 0 answer | 0 reply

[10:22 AM]
Mark A Delgado asked : Is there clarification on evidence documentation for proofing sessions, do electronic assertions must they be explicit or can they be implicit? (click through)
0 upvote | 0 answer | 0 reply

[10:24 AM]
Chris Edwards asked : Replacing legacy PACS (magstripe) in overseas facilities may take some considerable time yet...
0 upvote | 0 answer | 0 reply

[10:26 AM]
James Nicholas asked : We have plans to build a shippable enrollment station with a vendor that we'll send to end users to perform a remote supervised enrollment. Deploying KIOSK isn't feasible, especially for the speed of users NASA has. Can we ensure that FIPS accommodates solutions like these?

6 upvotes | 1 answer | 0 reply

Jim Fenton answered -
A "shippable enrollment station" sounds like an instance of what I referred to as a kiosk. Sorry if my use of "kiosk" gave a different impression. The important characteristic is that the equipment be issuer-controlled and that its integrity is assured.

[10:26 AM]
Cynetheia Brown (DOS) asked : Is SYM CAK being deprecated?
1 upvote | 1 answer | 0 reply

Justin Richer answered -
Yes, SYM CAK is deprecated in this version:
https://pages.nist.gov/FIPS201/authentication/#s-6-2-4

[10:26 AM]
Jon Luhman (SEC) asked : Just a comment - I know of at least one agency that scans the barcode for mustering/emergency accountability.
0 upvote | 1 answer | 1 reply

Jonathan Gloster answered -
barcodes still can be used optionally

Jon Luhman (SEC) replied -
I'll pass that along. Thanks!

[10:30 AM]
James Nicholas asked : Removing the CHUID completely eliminates flexibility for mustering and basic office/room access once one has already performed a strong auth to get in to a building. Can we simply put guidance out on usage instead of removing the capability?
4 upvotes | 1 answer | 1 reply

Andy Regenscheid (NIST) answered -
The CHUID data object will continue to be on the card. However, we're trying to clearly set expectations that you cannot rely on and use the CHUID as a secure authentication mechanism.

James Nicholas replied -
absolute, just wanted to make sure we can still use it where it makes sense. i.e. I just used PIV auth to get in a room with multiple offices. Now we can use CHUID to determine which office you can get in without performing another PKI operation on those doors within the room.

[10:38 AM]
Judith Spencer asked : Will implementation of SM-Auth have to wait until SP 800-74 is updated?
1 upvote | 1 answer | 0 reply

Andy Regenscheid (NIST) answered -
The SM-Auth will ultimately be specified in SP 800-73. Until that is updated, we won't have a fully-specified description SM-Auth, although obviously most of the details can be inferred from the existing language around secure messaging in the current SP 800-73. I think there could be value in some development/prototyping during the SP 800-73 revision process. Please reach out to us if you have specific ideas, questions or concerns.

[10:39 AM]
Stoicho GIzdov (LS3) asked : Is SM-AUTH intended to be used only in the context of OCC-Auth? Are there any other use cases?
0 upvote | 1 answer | 0 reply

Hildy Ferraiolo answered -
It can be used by itself as an authentication mechanism (SM-AUTH).

[10:40 AM]
Glen Lee (LANL) asked : What are the definitions of "Local Workstation Environment" and "Remote/Network System Environment"?

What's the intent of the AAL3 line item of the table? Does this mean that you can only use BIO-A and OCC-Auth to access a standalone computer, but you can't use it for network logon or access to o
2 upvotes | 0 answer | 0 reply

[10:43 AM]
David Florsek asked : Shouldn't PIN rejection also include phone number?

1 upvote | 1 answer | 1 reply

Jim Fenton answered -
There are a lot of other things we could disallow, and it's kind of a slippery slope. We're focused on disallowing the really common choices and dealing with the rest by limiting the number of retries.

David Florsek replied -
Maybe NIST should do a study of the common choices. If I know your identity, ph# would likely be the most likely choice I'd guess

[10:43 AM]
Stoicho GIzdov (LS3) asked : What about comparing to othe PII data? Such as DOB, SSN?
0 upvote | 1 answer | 1 reply

Jim Fenton answered -
There are a lot of other things we could disallow, and it's kind of a slippery slope. We're focused on disallowing the really common choices and dealing with the rest by limiting the number of retries.

Stoicho GIzdov (LS3) replied -
As #David Florsek mentioned in his reply. a standardized protocol may need to be established for removing identity-bound, easily guessable attribute(s). Relying on the fact that someone would not know a birth date of a cardholder is not the best assumption. Even three attempts can be plenty, given the sophisticated social engineering techniques available and the proliferation of personal data on social networks...

[10:45 AM]
Yves Massard asked : for the weak PIN, why not use an algorithm like making sure the difference between characters is not constant?
e.g.: a simple algorithm can weed out PINs like 0000 1111 1234 4321. Having a simple set approach would be better approach and has been available in the industry for a long time.
2 upvotes | 1 answer | 0 reply

Jim Fenton answered -
We're focusing on eliminating the really common choices, and dealing with the rest by limits on the number of retries allowed.

[10:46 AM]
Roger Roehr asked : Will SP 800-73 be changed so that people can not change the PIN with Middle ware?

1 upvote | 1 answer | 0 reply

Hildy Ferraiolo answered -
Hi Roger,
We will address this in SP 800-73 - taking in comments from stakeholder input wrt pro/cons.

[10:47 AM]
Tim Baldridge asked : The implication of the weak PIN requirement is that the CARD itself blocks such use. This implies a change to the PIV stock supply chain. It this the intention?

6 upvotes | 1 answer | 1 reply

Hildy Ferraiolo answered -
Hi Tim, Cards can do that today, to my knowledge.

Tim Baldridge replied -
Will the NIST NPIVP be updated to validate supplier smartcard stock and applets for this new FIPS 201 requirement. Would there be a grandfathering of existing, otherwise compliant, suppliers? and for how long?

[11:09 AM]
Adam Zeimet (USDA) asked : when we say "PIV issuer" in this DPIV use case, are we saying "home issuing agency" or the PIV CMS? In other words, in the case of a shared service provider like USAccess are we saying GSA\USAccess would have to manage the DPC?
12 upvotes | 0 answer | 0 reply

[11:11 AM]
Adam Zeimet (USDA) asked : ... If so, I would argue that the home agency identity management system (& CDM MUR) is the best place to manage this relation, not a PIV CMS
4 upvotes | 1 answer | 0 reply

Jonathan Gloster answered -
We will address in Q&A session

[11:11 AM]
Chris Edwards asked : When you say the Issuer, do you mean the Issuing Agency or the Issuing Service? e.g. can an Agency using the GSA MSO set up their own DPC issuing system?

3 upvotes | 0 answer | 0 reply

[11:13 AM]
James Belcher asked : Will SP 800-157 allow secondary authenticators to be administratively assigned to the PIV Account rather than requiring use of the PIV Auth to request the DPC? E.g. an OTP/SecureID authenticator that is provisioned to a MDM enrolled device.
2 upvotes | 0 answer | 0 reply

[11:14 AM]
Yves Massard asked : Why does the AAL3 column in slide 63 requires a password to get to

AAL3 with FIDO? FIDO2 and Webauthn can require the use of a PIN verified on the FIDO device just like a PIV card does and that means it should not require an additional password.
3 upvotes | 1 answer | 1 reply

Jim Fenton answered -
That's correct; the password could be either provided to the relying party (as with FIDO U2F) or to the authenticator (FIDO2). FIDO2 can do biometric activation as well.

Yves Massard replied -
thanks, hopefully the language in the special publication will make this clear so people don't assume that to get to AAL 3 with FIDO you need an additional password.

[11:14 AM]
Glen Lee (LANL) asked : What's the value proposition of having a "PIV Derived Credential" at a particular AALx per FIPS 201-3, versus implementing a derived credential capability the uses the PIV as the parent credential in accordance with 800-63A.
1 upvote | 1 answer | 1 reply

Jim Fenton answered -
Value proposition is that a wider range of authenticators can be used, not just PKI-based authenticators.

Glen Lee (LANL) replied -
Clarification. FIPS 201-3 says the DPC must be issued by PIV Issuer. But i can implement a Derived credentialing capability in accordance of 800-63 in my home agency that uses GSA as the issuer of PIV. But it is based on PIV thus is derived. What do i get with DPC that i don't get with DC?

[11:16 AM]
Farhan Saifudin (MobileIron) asked : Is there explicit guidance on how DPCs should be handled (stored/managed) on GFE managed devices vs BYO devices?
3 upvotes | 0 answer | 0 reply

[11:18 AM]
Lisa Palma asked : Expand on HW based Derived Cred... does this translate to a compliant 800-157 DPC with approved MDMs ;pushing the cert down to the native key store FIPS 140-2/3 cryptographic module , meaning no air gaps...is this was your confirming to a HW Based DPC
0 upvote | 1 answer | 0 reply

Jim Fenton answered -
Perhaps; FIPS 140 validation for mobile devices has been a challenge because of the rapid

changes in software versions.

[11:26 AM]
Mahan Talebian asked : Are there plans/use cases to expand DPC alternative authenticators to be issued to PIV eligible employees (successful NACI), who have yet to be issued a PIV card due to COVID restrictions?
3 upvotes | 2 answers | 0 reply

Jim Fenton answered -
As with other derived PIV credentials, the binding of the new alternative authenticators is planned to require first authenticating with the PIV. So PIV issuance would need to happen first. But if there's a strong need for this capability, that would be a good comment to make.

David Temoshok answered -
The requirement for In-person identity proofing for PIV enrollment (for IAL3 identity proofing in SP 800-63A) is not changed in rev.3. The new requirements and controls for supervised remote identity proofing allow for remote proofing to meet comparable assurance to in-person proofing.

[11:26 AM]
Brandon Meyer - USDA asked : Any rough timeline on a new 800-157 draft?
2 upvotes | 1 answer | 0 reply

Hildy Ferraiolo answered -
This will be covered in the 12:00 pm session.

[11:26 AM]
Carl Wallace asked : I don't think I heard face-to-face vetting mentioned. Is that still to be a requirement for AAL3?
2 upvotes | 4 answers | 1 reply

Jim Fenton answered -
That sounds more like an identity proofing requirement, so IAL3. Either in-person or supervised remote identity proofing discussed earlier are required at IAL3.

Hildy Ferraiolo answered -
It is still required in SP 800-157, but it could potentially change -- pending SP800-157 revision and alignment to SP 800-63.

Andy Regenscheid (NIST) answered -
FIPS 201-3 includes high-level requirements for how additional authenticators can be

bound to an existing PIV Account.

Simply put, additional authenticators can be bound to your PIV Identity Account remotely after you've succesfully authenticated with a PIV credential. There is a requirement to notify cardholders when an additional authenticator is bound to your account.

Andy Regenscheid (NIST) answered -
This is a bit of change from LoA-4 Derived PIV Credentials under the existing SP 800-157. LoA-4 DPCs effectively needed to be done in-person to meet the issuance requirements.

Carl Wallace replied -
There's a bit of a gap for hardware modules in the leap to AAL3 due to that requirement. We're getting much closer to (attested) hardware everywhere and the face-to-face requirement is a drag on asserting some OIDs.

[11:31 AM]
Mark Dale asked : OMB 19-17 states "Develop guidance to facilitate use ... of derived credentials for logical AND PHYSICAL access". FIPS 201-3, Section 3.1.3 addresses logical AND physical access along with PIV and derived credentials. Does this imply that derived credentials can be used for physical access?
2 upvotes | 1 answer | 1 reply

Hildy Ferraiolo answered -
Based on business requirement meeting with federal stakeholder, we did not hear uptake to use DPC for physical access. Hence, the PIV card is still status quo for PACS. We welcome further comment.

Mark Dale replied -
Thanks, Hildy! Understood. We would like to track that, and there will be follow up on that.

[11:31 AM]
Michael Lawlor asked : YES! SP for Federation is overdue!
1 upvote | 0 answer | 0 reply

[11:31 AM]
Camey Trossbach asked : Can you provide an examples of Federation use cases currently be employed in the fed space?

0 upvote | 1 answer | 2 replies

Andy Regenscheid (NIST) answered -
Enterprise applications at agencies frequently use federation protocols to integrate with the agency's single-sign-on system.

Some agencies use federation to integrate shared services with agency single-sign-on systems. For example, the National Finance Center, or even Max.gov (if you're not directly using your PIV card there).

Furthermore, federation protocols are very, very frequently used to integrate with cloud services. e.g., Office 365, Gsuite, WebEx. etc.

Camey Trossbach replied -
Thanks Andy

Camey Trossbach replied -
Where can I direct follow-up questions?

[11:32 AM]
Hussain Jafri asked : New publication of Derived PIV?

1 upvote | 1 answer | 0 reply

Andy Regenscheid (NIST) answered -
New guidelines on Derived PIV will be included in a revision to SP 800-157

[11:32 AM]
Michele Cohen asked : Can derived PIV be used externally to better protect PII like bio metrics

0 upvote | 0 answer | 0 reply

[11:33 AM]
Jim Thomson, MITRE asked : I would hope that a PIV Federation SP would be general enough to apply on other networks (fabrics), such as the Secret network (SIPR). Every federal network has this challenge, including the [DoD] partner networks.
0 upvote | 1 answer | 2 replies

Hildy Ferraiolo answered -
Noted. We do not have control over who will pick up the specification outside of PIV.

Jim Thomson, MITRE replied -
I look at it from the other way around, Hilde. A general SP with DoD and IC feedback, maybe with a PI-focused appendix. The practical neeed is to have common software for our ICAM programs. The governance challenge is that a more general SP can be required to be adhered to. A PIV-centric document cannot be mandated for other fabrics - or even the CAC, maybe.

--Jim

Jim Thomson, MITRE replied -
Opps! Hildy!

[11:34 AM]
Tim Baldridge asked : Will the new PIV Federation SP address concerns such as Holder of Key/Proof of Possession and Bearer assertion risks?

5 upvotes | 1 answer | 0 reply

Andy Regenscheid (NIST) answered -
There's an underlying assumption there that your applications need FAL-3 in the first place. In many cases, FAL1 or FAL2 will be sufficient.

But yes, we do see a need for more work on proof-of-possession assertions. Much of that work will not be done in the PIV suite of publications, but rather in SP 800-63C and industry standards.

[11:34 AM]
Timothy Schmoyer asked : If I use a federation protocol within the same organization, is it still FAL even though there are not different sovereign organizations PIV issuers.
2 upvotes | 2 answers | 1 reply

Jim Fenton answered -
One important characteristic is that all DPCs need to be invalidated when the PIV is terminated. Within the same organization, it depends on how closely the relying party and the PIV account are coordinated. Federation is a good way to do this within the organization as well.

Timothy Schmoyer replied -
I agree, federation protocols rock, but should I use FAL or IAL/AAL within the organization?

Justin Richer answered -
FAL, IAL, and AAL are all different dimensions of the system and would be used together.

[11:38 AM]
Hussain Jafri asked : Can an assertion be used for detailing Feds from one agency to another for a limited time?
0 upvote | 1 answer | 0 reply

Justin Richer answered -

Yes, assertions can be used for temporary assignments. An assertion is a very time-limited message that communicates a single authentication event.

[11:41 AM]
Timothy Schmoyer asked : UID could be either UUID 14 digits or the last 16 digits of FASC-N?
Organization UID (DoD ID, VA SecID, etc.)
Organizational Category
Organizational Identifier
Person/Organization Identifier
0 upvote | 0 answer | 0 reply

[11:41 AM]
Bill Price asked : How does RP know assertion was based on PIV authentication. There is nothing explicit about the initial PIV based authentication in the illustrated assertion.
0 upvote | 1 answer | 0 reply

Justin Richer answered -
Don't read too much into what I could fit into the examples on screen. :)

The federation SP will go into communicating that, and doing so in a trustable way. One possible technology is Vectors of Trust (RFC8485).

[11:43 AM]
Glen Lee (LANL) asked : Requiring the PIV Issuer to also be the IdP in this federation construct seems to impact agencies who are customers of GSA USAccess yet invested in an agency enterprise federation solution where it's the IdP for SPs.for federating authentication. Seems like a tall order for GSA to provide?

2 upvotes | 1 answer | 0 reply

Andy Regenscheid (NIST) answered -
There's a terminology challenge here. "Issuer" here primarily refers to the agency responsible for the cardholder. It does not preclude agencies from "outsourcing" certain aspects to shared services, or in-sourcing other aspects.

[11:44 AM]
Stephen Howard asked : SP800-73-4 now introduces (optional) Card Holder UUID. A long lived, "worldwide" identifier for a person. Might that be relevant in this discussion around Federation?
1 upvote | 2 answers | 1 reply

Justin Richer answered -

The Chardholder UUID would help identify the account to the IdP, but the IdP needs to be able to create an identifier for speciifc RP's where needed so it can't be relied upon for all cases. Additionally, since it's an optional identifier it can't be relied on for all accounts.

Subject identifiers are required for federation assertions, and it's up to the IdP to make sure the combination of (user + RP) maps to a consistent identifier.

Stephen Howard replied -
I hear you. Been there, worked on that. Identity mapping between IdP to RP can certainly involve unique identifiers. Yet in the Federal Enterprise, we tend to want to really know who we are talking about, both as IDP and as multiple RPs so we can manage things like insider threat or CDM. fostering a unique identifier on a per RP basis is counter to those initiatives. I support both, but would still recommend using Person UUID as much as possible.

Justin Richer answered -
800-63C allows the IdP to divulge mapping in cases of security threat, to mitigate exactly that.

[11:46 AM]
Mark Russell asked : The FIPS pub may not be the right venue, but some guidance on the special case of using other-agency PIV for desktop login would be helpful
1 upvote | 0 answer | 0 reply

[11:46 AM]
Timothy Schmoyer asked : identifier syntax for federation?
RFC 4122 128 bits
Existing 10 digit UIDs in organizations
16 digit Person|OC|OI|POA
0 upvote | 0 answer | 0 reply

[11:49 AM]
Ross Foard (CISA) asked : Thank you Justin for going where only the brave venture.
6 upvotes | 0 answer | 0 reply

[11:49 AM]
Timothy Schmoyer asked : Session Management using mutual TLS and Holder-of-Key?
0 upvote | 0 answer | 0 reply

[11:51 AM]
Glen Lee (LANL) asked : FIPS are considered policy and "thou shall do". By putting PIV Federation requirements in the FIPS (versus an SP), how do we combat pressures by auditors who question why our perfectly appropriate (and acceptable) federation approach

is not in accordance with FIPS 201-3.
4 upvotes | 1 answer | 2 replies

Jonathan Gloster answered -
FIS201-3 will reference a Federation SP for requirements

Glen Lee (LANL) replied -
Great. Though i don't see it in the list Hildy is presenting as a new SP that will be developed

Glen Lee (LANL) replied -
i retract my last comments. slide 120 covers it on the last line item of the table. :)

[11:51 AM]
Stephen Howard asked : Session management, in my experience, has a lot of difficulty establishing holder of key/session relationship to achieve high assurance. Especially as the session relies on multiple transactions over the session. Does this suggest a solution?
4 upvotes | 1 answer | 0 reply

Justin Richer answered -
Holder of key would be used in establishing the session. Maintenance of the session is a separate question, and is handled in SP 800-63B's session management discussion.

[12:03 PM]
James Belcher asked : Will the implementation schedule for the new mandatory and removed features in FIPS 201-3 standard have a similar 12 month implementation period that was provided in FIPS 201-2?
2 upvotes | 0 answer | 0 reply

[12:11 PM]
Martin Baltiyski asked : According to 800-63, there are only 4 types of authenticators that can achieve AAL 2 or 3 on their own. Does FIPS 201-3 allow only those to be issued as derived credentials?
3 upvotes | 1 answer | 0 reply

Jim Fenton answered -
Single-factor authenticators used in conjunction with another factor (typically memorized secrets) can also be used.

[12:11 PM]
Michele Cohen asked : Standard seems to be highly dependent on other guidance including one that hasn't been fully explained like Federation

1 upvote | 0 answer | 0 reply

[12:12 PM]
Ross Foard (CISA) asked : Hildy was clear about what's in and out of scope for this review. Is there a plan to open up referenced/dependent SPs for comment so we can address comment to the appropriate doc?
0 upvote | 0 answer | 0 reply

[12:13 PM]
James Belcher asked : Can a Supervised Remote ID Proofing station be used for the dual purpose of registration and issuance if cardstock is controlled by the on-site staff that manage the station?
0 upvote | 1 answer | 0 reply

Jim Fenton answered -
In principle, yes, if the requirements for accountability of cardstock, etc. can be met and the station has the capability to personalize the card. This probably puts more requirements on the staff (guard) that are co-located with the station.

[12:15 PM]
Michael Lawlor asked : a remote PIV app (virtual KIOSK) could also be used for resetting PINs when physical access isn't realistic

2 upvotes | 0 answer | 0 reply

[12:17 PM]
robert schlecht asked : [12:13 PM] Schlecht, Robert [USA]

Let me restate the question: When leveraging a Proxy or Broker model for agency enterprise federation service,how can an RP guarantee the user logged on with PIV-Auth at the CSP? Under the Proxy federation model, our agency will have the user present their PI
1 upvote | 1 answer | 1 reply

Justin Richer answered -
The proxy has to trust what the inbound IdP asserts. The RP has to trust what the RP asserts. This is why we're defining PIV Federation in terms of a canonical IdP, so we can determine the trust metrics associated with it.

robert schlecht replied -
By default FAL1 (signing) is used to establish trust. Trust exists throughout the flows (IDP-Proxy-RP). The issue is no generic/standard attribute and value exits for PIV-Auth, only smartcard. Hence, Cybersecurity requires user to authentication (TSL / PKI-Auth) to an agency Web Server, which then does federation (SAML) to the RP.

[12:20 PM]
Martin Baltiyski asked : The term Account or Identity, or even worse, Identity Account, seems inappropriate in the PIV context, and is likely to cause much more confusion. If you call something X, but then you have to explain to your audience that it is not the X that they typically think of, then it is not really X, but Y.
4 upvotes | 0 answer | 0 reply

[12:20 PM]
Bill Windsor asked : Would it be possible to setup a follow up discussion on person identifiers with DHS - would like to include Andy, Justin and Hildy at a minimum?

2 upvotes | 0 answer | 0 reply

[12:20 PM]
Glen Lee (LANL) asked : so the expectation of the IdP is that it must know and manage the userIDs for all RPs that use the IdP?
2 upvotes | 3 answers | 1 reply

Justin Richer answered -
Effectively yes, but they aren't user-facing identifiers so they can be derived. One thing I've seen in practice is a hash function that takes in the account identifier and RP, as well as mixed with a secret known to the IdP only.
Glen Lee (LANL) replied -
Ouch. Account managment nightmare is now been thrust to the IdP. Hard enough for individual RPs to do, now it's a factor of N RPs for the IdP itself. Can't wait for the SP to tell me how i can do this in practice.

Justin Richer answered -
The IdP's entire job is account management, it's a specialized service. An RP only does account management because it has to in order to allow people to access functionality.

Justin Richer answered -
As a corrollary, the federation model allows the RPs to not deal with account management nearly as much as they are forced to when federation is not used.

[12:21 PM]
David Florsek asked : wrt Robert's question what about providing evidence of PIV usage what about information about MFA as well?

0 upvote | 1 answer | 0 reply

Jim Fenton answered -
As Justin indicated, there are standards for conveying the AAL of the authentication process.

Anything more fine-grained would require a more proprietary approach.

[12:23 PM]
Stephen Howard asked : There has been recent guidance on Enterprise IDMS tracking Digital Workers (e.g., AI, ML, ...). Is this a concern in the FIPS 201 space?
2 upvotes | 0 answer | 0 reply

[12:24 PM]
Tim Baldridge asked : How are PIV Federation provider services envisioned, will it follow the GSA U.S. Access credential issuer model for PIV Cards? Clearly larger Depts. and Agencies may do their own, but there are many smaller ones that may outsource, but to whom?

2 upvotes | 0 answer | 0 reply

[12:26 PM]
Bill Price asked : Are the cloud service and major SaaS providers such as MS Office and 365, Google Docs involved? It would be nice if they would accept Federation assertions?
0 upvote | 1 answer | 1 reply

Andy Regenscheid answered -
Federation is already being widely used to integrate cloud services with agency single-sign-on systems.

Bill Price replied -
True but they may currently accept weak assertions that pose a security risk.

[12:27 PM]
Timothy Schmoyer asked : Can you clarify: ""Issuer" here primarily refers to the agency responsible for the cardholder. It does not preclude agencies from "outsourcing" certain aspects to shared services, or in-sourcing other aspects."
This means GSA issued PIV Card, but GSA is not the issuer because DHS owns the cardholder
1 upvote | 1 answer | 3 replies

Jim Fenton answered -
"Issuer" is perhaps a bit of a confusing term. We're generally talking about the agency that maintains the user's PIV account/enrollment record.

Timothy Schmoyer replied -
So GSA is the "issuer" maintaining the cardholder's PIV account/enrollment record in the GSA IDMS for DHS owned PIV cardholders.

Timothy Schmoyer replied -
However, DHS is the authority for issuing the PIV card from GSA to the DHS owned cardholder.

Timothy Schmoyer replied -
DHS is the also the authority for revoking the PIV card, by collecting the card and notifying GSA for certificate revocation?

[12:29 PM]
Timothy Schmoyer asked : How does GSA IDMS correlate identifiers on/in the PIV with issuer identifiers?
0 upvote | 0 answer | 0 reply

[12:30 PM]
Chris Edwards asked : We have a similar problem with PIN reset being done from a remote user's workstation, connected to the CMS over UPN for example. At present section 2.9.3 would appear to preclude self-service PIN reset using biometric verification at the user's desktop, yet we allow Biometric PIN.
0 upvote | 0 answer | 0 reply

[12:30 PM]
Chris Edwards asked : (VPN)

0 upvote | 0 answer | 0 reply

[12:32 PM]
Stephen Howard asked : Adding an individual to "man" the SRIP environment re-introduces the problems of an Enrollment Official like model. Seems counterintuitive to the whole concept of a tamper evident suite of tools (kiosk and others) that meet current SP800-63A requirements. What is driving the need for monitoring?
3 upvotes | 1 answer | 0 reply

Jim Fenton answered -
Level of supervision required of course depends on the tamper protections that the SRIP station has. But it seems like a bit of a stretch for it to be completely unattended -- on a street corner, in a shopping mall, etc.

[12:32 PM]
Roger Roehr asked : Would live video observation be authorized for remote proofing?
1 upvote | 0 answer | 0 reply

[12:33 PM]
Yves Massard asked : Agreed with Stephen, especially since there is a remote enrollment

officer that already witnesses the enrollment and the overview camera is already supposed to capture the enrollment devices as well as the applicant in one single frame.
0 upvote | 0 answer | 0 reply

[12:40 PM]
Michael Lawlor asked : Like NT Technology? :-)

2 upvotes | 0 answer | 0 reply

[12:42 PM]
Martin Baltiyski asked : What is the difference between PIV Account and an account on AD that is enabled for PIV card login. Using the same term in PIV is going to cause a lot of confusion.
1 upvote | 0 answer | 0 reply

[12:44 PM]
Tim Baldridge asked : What does it mean to have a PIV Identity account, consider multiple personas/affiliations within one agency and then the cross-agency use cases. There exists today legitimate cases for issuing multiple PIV Cards to a single individual, is this one PIV account or multiple PIV accounts for PIV card?
1 upvote | 0 answer | 0 reply

[12:46 PM]
Ross Foard (CISA) asked : Clarifying the terms will help. In 800-63-3a there is at least one paragraph that uses the term derived PIV and PIV-derived in the same paragraph, the first used to describe the capability and the second identifying a reference to (oddly) the SP 800-157 guidelines.
0 upvote | 2 answers | 0 reply

Jim Fenton answered -
We will need to consider the broadening of derived PIV credentials in the (currently in progress) revision of the SP 800-63 suite. This is an informative section so it's only giving examples.

Andy Regenscheid answered -
The fact that we're doing the updates to SP 800-63 and FIPS 201 will give us an opporuntity to clean up some of the language. Including around derived credentials and derived PIV credentials.

[12:48 PM]
Timothy Schmoyer asked : If enrollment record information is spread between CSP issuers, organizational IdMS, organizational IdPs, etc., how does that help federation across govt?

1 upvote | 3 answers | 2 replies

Andy Regenscheid answered -
Not all enrollment data would need to be shared. In fact, I think very little would need to be shared. The assertions conveys via federation mainly need to include sufficient identity attributes to identify a particular user. These would need to be available to the IdP, and likely consolidated in the enteprise IDMS

Jim Fenton answered -
The intent is to centralize enrollment record information at the organizational CSP. Federation is used to make that possible, and does require that the information be coordinated with the organization's IdP. But everything outside the agency should be handled by federation.

Timothy Schmoyer replied -
I think this directly impacts DoD Mission Partner Registry and DoD Mission Partner Exchange as well as the DHS efforts for PIV/CAC interoperability/federation.

Timothy Schmoyer replied -
DHS using GSA issued PIV and DoD using legacy CAC.

Jim Fenton answered -
Remember that the federation is specifically required for non-PKI derived credentials/authenticators. Current interagency use of PIV is the same as it is now.

[12:48 PM]
Bill Price asked : Some agencies are currently issuing credentials that leverage the identity proofing of PIV cards but would not meet the requirements for a DPC. What are the controls on issuing FPKI certs that assert the Derived PIV policy? Are only CSPs allowed to request certs with that policy?
0 upvote | 1 answer | 1 reply

Justin Richer answered -
This isn't a full answer to the question, but note the updated definition of derived PIV means that there are derived PIV credentials that aren't PKI or certificate based.

Bill Price replied -
Understand but still interested in what restrictions would apply to certs for PKI based credentials that use PIV for id proofing. Can the certs be issued under FPKI? What cert policies?