Internet Printing Protocol Meeting Minutes
February 7-9, 2023

Meeting was called to order at 10:45am EST on February 7, 10:00am EST on February 8, and 12:45pm EST on February 9, 2023.

Attendees

Taiki Arai (OkiData)
Graydon Dodson (Lexmark)
Benjamin Gordon (Google)
Smith Kennedy (HP)
Jeremy Leber (Lexmark)
Ira McDonald (High North)
Piotr Pawliczek (Google)
Anthony Suarez (Kyocera)
Michael Sweet (Lakeside Robotics)
Paul Tykodi (TCS)
Bill Wagner (TIC)
Steven Young (Canon)

Agenda Items

1. Antitrust and IP policies, minute taker
    - https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf
    - https://www.pwg.org/chair/membership_docs/pwg-antitrust-policy.pdf
    - Antitrust and IP policies accepted, Mike taking minutes
2. Status:
    - https://ftp.pwg.org/pub/pwg/ipp/slides/ipp-wg-agenda-february-23.pdf
    - Call for Objections: IPP Job Extensions v2.1 (JOBEXT)
        - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippjobext21-20221212-rev.pdf
    - Formal Vote: IPP Driver Replacement Extensions v2.0 (NODRIVER)
        - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippnodriver20-20230121.pdf
    - Finished at 11:20
3. IPP/2.0
    - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippbase23-20220809.pdf
    - Waiting on JOBEXT and EPX to issue prototype draft
4. IPP Everywhere v2.0
    - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippeve20-20221107.pdf
    - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippeveselfcert20-20220510-rev.pdf
    - Smith: Would be nice to front-load some of the product testing, can we do some slides highlighting the changes?
        - Mike: Yes, can also have ipptool test files available sooner
        - Smith volunteers to do IPP Everywhere 2.0 slides, Mike will do test

files

- Action: Smith to create IPP Everywhere 2.0 slides showing changes
- Action: Mike to update IPP Everywhere 2.0 test files

- Mike: Existing clients typically already support optional/recommended IPP Everywhere 1.1, so only new 2.0 stuff such as job-triggers in NODRIVER will need new code to support
- Smith: Can we have PDF spec links to sections/items?
    - Mike: PDF URLs can have page references, other things not so much
- Smith: Can we have a presentation/overview of Github repository changes in May?
    - Mike: Sure
- Smith: Any issues getting Flutter apps approved on the various stores?
    - Mike: No, still native code underneath.
- Smith: Can we use Dart to prototype other IPP things?
    - Mike: Yes, but certain items might be better prototyped in CUPS, PAPPL, etc.
- Flutter/Dart code is currently in the "flutter" branch, will be merged to master in near future
- Finished at 1:45

5. Prototype-Ready Specifications
    - IPP Encrypted Jobs and Documents:
        - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ipptrustnoone10-20210519-rev.pdf
        - Bill: 2 years old, should we review again before more prototyping?
            - Yes, but put together a list of topics to get the most from it
        - Smith: Want to review use cases - make sure Client can control decryption since Printer isn't trustworthy?
            - Mike: Can reuse TLS X.509 certs for direct hops, also want to talk more about cert validation
            - Ira: Like we are talking about for OAuth
        - Mike: Also talk about integrity (signing without encryption) use case - important for 3D printing
    - IPP Enterprise Printing Extensions v2.0 (EPX)
        - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippepx20-20230206-rev.pdf
        - Section 3.1, Drop "Also, " before "Given"
        - Global: check for broken cross references
        - Figure 5: Tweak withe copies and resume-job are on the same side?
        - Figure 12: Missing some arrows
        - Global: Make sure "Authenticated User" is properly capitalized throughout
        - Section 6.1.4.3: Flip around - Printer MUST reject vs. Client MUST supply
            - Global: Check for Client MUST - normally Printer MUST
        - Section 6.4.5: job-password-repertoire-configured should be "type2 keyword | no-value"

        - Section 6.4.14: printer-asset-tag should be "octetString(MAX) I no-value"
            - The 'no-value' out-of-band value indicates that no asset tag value has been set.
        - Section 6.4.18: Fix paragraphs and style at end
        - Section 6.4.19: "MUST have the value 'automatic' or 'spool'." (job-spooling-supported is single-valued)
        - printer-storage-xxx are Printer Status attributes
        - Note for NODRIVER: printer-input-tray and printer-output-tray should be Printer Status attributes, check for others offline
        - Stopped at section 7, will resume in next week's concall

6. Evolution of OAuth and IPP
    - https://github.com/istopwg/ippsample/wiki/IPP-and-OAuth
    - https://ftp.pwg.org/pub/pwg/ipp/whitepaper/google-pwg_user_identity.pdf
    - https://ftp.pwg.org/pub/pwg/ipp/whitepaper/google-pwg-trust.pdf
    - https://datatracker.ietf.org/doc/draft-sweet-iot-acme/
    - Smith: What is IETF doing for trust/attestation?
        - Mike: Current "state of the art" is to maintain a "curated" list of trusted manufacturer root certificates
    - Smith: Can we just have the cloud registration generate a trusted X.509 cert for the printer?
        - Piotr: Could also set mDNS name to a globally-unique value and include that in the certificate?
        - Mike: Microsoft's UPS uses CSRs in the provisioning process to get a trusted X.509 cert
        - Mike: mDNS hostnames can get conflicts due to "reflections" when network segments re-connect, which can lead to renaming even for unique names
    - Mike: Need to be flexible, local sites will define actual policy
    - Smith: Seems like some of the requirements are fuzzy
        - Mike: Think we are agreed on no self-signed certs, but lots of options on getting CA-signed certs
        - Smith: A lot of IoT attestation depends on manufacturer-supplied (from factory) certificate
            - Mike: Not comfortable with factory certificates - not a great track record on private key security and expiring certificates enforce a shelf life
        - Smith: Joining OAuth requires CA-Signed certs?
            - Piotr: Admin should be able to set cert on printer
            - Mike: Might use X.509 certs to authenticate between Printer and AUTHZ and IP
        - Benjamin: Can we use printer-uuid
            - Mike: Not authenticated, can be impersonated
    - How to securely connect to network and ensure that we aren't talking to a malicious printer?
        - Mike: NEA/TNC (Trusted Network Connect)
        - Mike: Everything depends on having a trustworthy X.509 certificate

        - Public CA: OK
        - Private CA: probably OK, some limitations for automatic issuance
        - Self-signed: vulnerable to time-of-use
    - Smith: How to validate that printer is trusted by AUTHZ?
        - Piotr: List of trusted AUTHZ servers on Client
        - Smith: Then printer shouldn't provide attribute then?
            - Piotr/Mike: Can have multiple AUTHZs, attribute specifies which one
        - Smith: Can certificate specify AUTHZ?
            - Piotr: No, admin has to set things up on the printer
        - Smith: Need concrete examples and less hand waving
- Google PWG Trust white paper:
    - Not sure how to get private CA root certificate loaded on printer? Do printers support this for things like Microsoft Universal Print Service???
        - Mike/Piotr: Hope they validate X.509 certs when connecting to cloud services
    - Mike: Important to allow installing private root certificates on a printer to allow Printers to validate services that it connects to
        - Call out to members: what do your printers currently support for trusted root certificates
    - Piotr: Do we want to allow self-signed certs?
        - Mike: No, want greater security
        - Drop "other certificate" from Client->Printer table
    - mDNS hostnames are typically vendor prefix + MAC address - local address conflicts should be rare out of the box
        - Smith: User is able to change the mDNS hostname which might not be as unique
        - Smith: What about CNAMEs and mDNS?
            - Mike: I don't think they are allowed, will check
    - How to setup certificates for mDNS (.local) hostnames?
        - Mike: ACME IoT, ActiveDirectory, Cisco, etc.
        - Provide recommendations on naming (if you have to, include unique identifier like MAC address in .local hostname, but recommend site-unique domain name)
        - Provide recommendation on what printer URI to use with OAuth
    - AUTHZ to Printer: Need to define how Token Introspection request is authenticated (can't just send token for decoding - needs to come from authorized printer)
    - Piotr: Why use cloud access control with home printers?
        - Mike: Some use cases where employer needs to record all print jobs for legal reasons, but that is a cloud configuration
        - Smith: Also "licensed/subscription" printing features for local printers
    - Piotr: How does Microsoft UPS work?

- Mike: Printers, users, etc. all tied to ActiveDirectory domain name

- Google PWG User Identity white paper:
  - Mike: Need to extract Authenticated User from token "sub" value
  - Possible to determine whether Printer needs to use token introspection by looking at metadata
  - Can assume that Printer needs user identity when OAuth is configured
  - Can assume the Printer can get the Authenticated User from the "sub" value
- RAR vs. Scopes
  - Access token already has identity ("sub")
  - Access level defined by identity
  - "oauth-authorization-scope" means use scopes
  - "oauth-types-supported" (oauth-authorization-type-supported?) means use RAR
  - "oauth-groups" (oauth-authorization-group-supported?) lists named groups for printing
    - Mike: Are groups less opaque than scopes?
  - Scopes == 2 round trips the first time, 1 per printer afterwards (with the same AUTHZ and scopes)
  - RAR == 3 round trips the first time, 1 per printer afterwards (with the same AUTHZ and groups)
  - Mike: Are there existing implementations of RAR?
    - Piotr: I don't think so
  - Will come back to this in the next concall
- Also discuss JWE/JWS at the next concall (on the wiki)

7. 3D Printing
   - Ira: MQTT is an unreliable message delivery protocol (like sending an SMS) - no authentication, message integrity, or encryption
   - Smith: Should probably look at the status/eventing/notification facilities in the 3D space
     - Paul: Existing architecture is perfect for remote 3D job submission and monitoring, but existing vendor APIs are limited; 3MF might want this but OPC UA/MT Connect are already doing something here
       - OPC UA is paid access specs/orgs, specs published through IEC
       - MT Connect is open access, specs published through ANSI
       - umati is open access
     - Mike: OPC UA/MT Connect are more machine control?
       - Paul: Yes
     - Mike: OK, so then IPP would sit on top of OPC UA/MT Connect and provide the higher level (common) data model and status information?
       - Paul: Yes, and this is something umati is working on/towards
       - Paul: This should also help with 3MF efforts

- One headache that isn't being talked about are file formats - no way to know what to send today with non-IPP solutions
    - That should change over time but all the different formats are a cause of issues today
- Paul: Industry is now starting to understand the relevance of/use for IPP 3D

Next Steps / Open Actions

- Next conference calls on February 16 and March 2, 2023 at 3pm
- Action: Smith to create IPP Everywhere 2.0 slides showing changes
- Action: Mike to update IPP Everywhere 2.0 test files