Internet Printing Protocol Meeting Minutes
August 16-18, 2022

Meeting was called to order at 10:45am EDT on August 16, 10am EDT on August 17, and 12:45pm EDT on August 18.

Attendees

Taiki Arai (Oki Data)
Benjamin Gordon (Google - ChromeOS)
Amitha Kundapur (Konica Minolta)
Smith Kennedy (HP)
Jeremy Leber (Lexmark)
Ira McDonald (High North)
Piotr Pawliczek (Google - ChromeOS)
Michael Rhines (Qualcomm)
Anthony Suarez (Kyocera)
Michael Sweet (Lakeside Robotics)
Bill Wagner (TCS)
Uli Wehner (Ricoh)
Jimmy Wu (Microsoft)
Steven Young (Canon)
Ray Xu (Google - ChromeOS)
Michael Ziller (Microsoft)

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-august-22.pdf
   - Action: Mike to start IPP WG Last Call on PPX until September 1
3. Job Extensions v2.1
   - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippjobext21-20220809-rev.pdf
   - Add line numbers
   - Section 4.4: Clarify last sentence to make it clear that preprocessing is being done before output, maybe mention potential confusion of date-time-at-processing for accounting?
   - Section 4.6: Add a note about deprecated Restart-Job and Reprocess-Job operations, which Resubmit-Job replaces
   - Section 6.3.1: Isn't media required by STD92?!?
   - Section 16.1: Fill out bullets
4. IPP/2.x

- https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippbase23-20220809-rev.pdf

5. IPP Everywhere 2.0
   - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippeve20-20220510-rev.pdf
   - https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippeveselfcert20-20220510-rev.pdf
   - Platforms to target:
     - Smith: We use all three platforms, main concern is how IPP-USB is exposed on each platform, still want command-line
     - Mike: Yes, still command-line tools bundled with GUI
     - Jeremy: Same here
     - No clear preference on platforms
   - Sample GUI:
     - Smith: Maybe add a way to add a calendar reminder for sending the JSON file?
     - Smith: Also show prior certs, whether they have been submitted, etc.
     - Mike: Maybe include a way to run a subset of tests, other common tests, print test files
6. 3D Printing/Liaisons
   - Slide 24: Add Safe G-Code Best Practice for current documents
   - ISO WG12 is now working on 3D scanning
   - VDMA - OPC UA investigating IPP work
     - IPP continues to be the only solution for secure remote/network submission of 3D content
     - UMATI (Universal Machine Technical Interface) may demo something at formnext in November
     - Not sure whether OPC UA efforts will be ready in time
     - Should know in 3-4 weeks
   - ISO / 3D PDF Consortium:
     - Now looking at adding glTF format (OpenGL format)
       - https://www.khronos.org/api/index_2017/gltf
       - https://github.com/KhronosGroup/glTF
       - https://github.khronos.org/glTF-Sample-Viewer-Release/
     - Also looking at where to put metadata - some describes the 3D content while other is specific to processing/intent and would usually be separate (i.e. IPP job ticket)
     - Also how to deal with different versions of PDF, different embedded content formats (e,g, STEP vs. other 3D content)
   - Transportation Research Board - will know in the next month whether we will present
7. IPP and OAuth
   - Resource identifiers
     - URI or octet string? What does OAuth spec say?
     - Benjamin: Can this be manually configured?
       - Mike: Yes, intent is for Clients to get the correct value automatically but Printers might need manual configuration
     - Ira: New UUID RFC is coming from IETF, new workgroup formed
       - Smith: Update NODRIVER to eliminate UUID length limits,

        - maybe add historical note about previous limits
    - Do we need multiple resource URIs, one per IPP endpoint? Specifically cloud vs. local for a printer discovered via company directory service with multiple endpoints?
        - Make "oauth-resource-uri (1setOf uri)" (multi-valued)
        - 1 value means all of the printer-uri/system-uri values use the same
        - N values means ordered list corresponding to printer-xri-supported/system-xri-supported
    - Piotr: Not sure merging local and cloud queues is a good design decision
        - Mike: But there are existing solutions that do just that, so we need that level of flexibility
    - Protr: Also man-in-the-middle attacks:
        - Separate resource URI allows an attacker to obtain an OAuth token for an authorized printer, and then either intercept or abuse access to the authorized printer
    - Don't have separate attribute for resource URI, need to use printer/system URI to ensure that authorization is only granted for the URI the Client is connecting to (security)
- TPM 2.0:
    - Platform identity device ID, generates local device ID derived from platform and network IDs
    - Platform certificate
    - Certification guarantees uniqueness, unique keys generated during manufacturing, certificate issued by trusted CA
    - Mike: What about certificate/key expiration/revocation?
        - Ira: Silent about revocation, root key is immutable, other keys can be regenerated
        - Ira will investigate limitations of certificate life time, renewal
    - TPM might be used to generate an X.509 certificate that would be more trustworthy than a self-signed cert (important to OAuth authorization flow to confirm identity of printer)
- How to know a printer is part of the local OAuth infrastructure?
    - "uri-authentication-supported" and "xri-authentication-supported" has 'oauth' in it
- How to associate a Printer with OAuth
- Man-in-the-middle attacks:
    - RFC 8693 token exchange uses a resource path to link the Client's OAuth token with a specific resource
    - RFC 7636 PKCE
        - https://auth0.com/docs/get-started/authentication-and-authorization-flow/authorization-code-flow-with-proof-key-for-code-exchange-pkce
    - How to verify the resource?
        - TLS server certificate validation only validates a good cert, not necessarily that the printer is the same

            - TLS negotiation: server certificate includes hostname that you connected to
            - How to verify that the OAuth server trusts the printer we just talked to?
                - Disallow self-signed certificates for printers that use OAuth?
                - But what about .local certificates issued by a local ACME server? How to prevent new devices from getting certificates for an existing hostname?
            - RFC 8693 doesn't validate Printer (resource) certificate, resource is OPTIONAL
    - Some trust is coming from other protocols/specs:
        - TLS and X.509: Printers need certs with trusted root certificates to prevent man-in-the-middle attacks
        - Need token exchange to validate that OAuth server knows about the printer URI
    - Security considerations for OAuth:
        - Don't allow self-signed certs (unless explicitly trusted/pinned) i.e. no TOFU for OAuth
        - Assumption is that TLS certificate validation + OAuth token exchange is enough to validate that a printer is known
    - Token exchange protects user credentials, lifespan can be limited
8. Next steps
    - Tiger team meetings for OAuth?
    - Continue discussions on IPP mailing list
        - TPM - certificates and keys, further investigation
        - PKCE
        - Device authorization grant
        - Scopes
        - Prototyping
        - Spec updates
    - Action: Mike to post IPP wiki page for OAuth to mailing list
    - Possible work with IDS

Next Steps / Open Actions

- Next conference calls on September 1 and 15, 2022 at 3pm
- Action: Mike to start IPP WG Last Call on PPX until September 1
- Action: Mike to post IPP wiki page for OAuth to mailing list
- Action: Mike to post announcement for approved IPP Finishings 3.0 document (DONE)
- Action: Mike to update IANA IPP registry for media-size syntax and range of values (DONE)
- Action: Smith to update PWG 5100.7 errata to note 1:MAX range of values (DONE)
- Action: Mike to put together a proposed UI for new self-cert tools (DONE)