The Printer Working Group

February 5, 2021
Best Practice 5199.11-2021

Job Accounting with IPP v1.0

Status: Approved

Abstract: This document discusses how to perform different kinds of job accounting with IPP and how to address privacy and consent issues associated with accounting information.

This is a PWG Best Practice. For a definition of a "PWG Best Practice", see:

https://ftp.pwg.org/pub/pwg/general/pwg-process30.pdf

This best practice is available electronically at:

https://ftp.pwg.org/pub/pwg/informational/bp-ippaccounting10-20210205-5199.11.docx
https://ftp.pwg.org/pub/pwg/informational/bp-ippaccounting10-20210205-5199.11.pdf

Title: J*ob Accounting with IPP v1.0*

Table of Contents

1. Introduction 5
2. Terminology 5
2.1 Conformance Terminology 5
2.2 Printing Terminology 5
2.3 Protocol Role Terminology 6
2.4 Acronyms and Organizations 7
3. Rationale 8
3.1 Use Cases 8
3.1.1 Audit Print Usage 8
3.1.2 Audit Print Content 8
3.1.3 Billing 8
3.1.4 Diagnosing and Debugging Printing Issues 8
3.1.5 Supplying Required Information 8
3.1.6 Supplying Optional Information 8
3.1.7 Authenticating End Users 9
3.1.8 Authenticating Print Services 9
3.1.9 Reconfiguring a Print Service 9
3.2 Exceptions 9
3.2.1 Opt-Out of Mandatory Data Collection 9
3.2.2 Opt-Out of Optional Data Collection 9
3.3 Out of Scope 10
3.4 Design Requirements 10
4. IPP Model for Job Accounting 11
4.1 Client Supplied Metadata 11
4.2 Printer Generated Metadata 12
4.3 Job Creation Requests and Recommended/Required Attributes 12
4.4 Explicit Consent 12
4.5 Privacy and Data Retention Policies 13
4.6 Data Validation 13
4.7 Authenticated Guests 14
5. Internationalization Considerations 15
6. Security Considerations 15
6.1 Client Considerations 15
6.2 Printer Considerations 16
6.3 Privacy and Data Collection 16
6.4 Data Protection 16
6.5 Data Validation 17
7. Common Job Accounting Metadata 18
8. References 19
9. Author's Address 21

List of Figures

Figure 1 - Example Explicit Consent Dialog 13

List of Tables

Table 1 - Common Job Accounting Metadata 18

1. Introduction

This document discusses how to perform different kinds of job accounting with IPP, including auditing of content and usage, billing, supply and service management, and diagnostics and debugging. In addition, this document provides guidance on the privacy and consent issues associated with the collection, storage, and processing of accounting information

2. Terminology

2.1 Conformance Terminology

Capitalized terms, such as MUST, MUST NOT, RECOMMENDED, REQUIRED, SHOULD, SHOULD NOT, MAY, and OPTIONAL, have special meaning relating to conformance as defined in Key words for use in RFCs to Indicate Requirement Levels [BCP14]. The term CONDITIONALLY REQUIRED is additionally defined for a conformance requirement that applies when a specified condition is true.

The term DEPRECATED is used for previously defined and approved protocol elements that SHOULD NOT be used or implemented. The term OBSOLETE is used for previously defined and approved protocol elements that MUST NOT be used or implemented.

2.2 Printing Terminology

Normative definitions and semantics of printing terms are imported from the Internet Printing Protocol/1.1 [STD92].

Administrator: An End User who is also authorized to manage all aspects of an Output Device or Printer, including creating the printer instances and controlling the authorization of other End Users and Operators [RFC2567].

Authenticated Guest: An End User who is authenticated and authorized to perform basic printing functions as a guest on the network. Guests are typically limited to using printers in common areas and granted access for a specific amount of time.

Client Supplied Metadata: All Job/Document Template and operation attributes supplied in a Job or Document Creation request.

Document: An object created and managed by a Printer that contains the description, processing, and status information. A Document object may have attached data and is bound to a single Job [STD92].

End User: A person or software process that is authorized to perform basic printing functions, including finding/locating a printer, creating a local instance of a printer, viewing printer status, viewing printer capabilities, submitting a print job, viewing print job status, and altering the attributes of a print job [RFC2567].

Job: An object created and managed by a Printer that contains description, processing, and status information. The Job also contains zero or more Document objects [STD92].

Job Accounting: Collection of Metadata to audit, bill, or otherwise report on the origin, processing, and disposition of Jobs and Documents.

Logical Device: A print server, software service, or gateway that processes jobs and either forwards or stores the processed job or uses one or more Physical Devices to render output [STD92].

Metadata: Information about a Job or Document such as name, originator, owner, format, state, counters, dates and times, content, and template attributes.

Operator: An End User that also has special rights on the Output Device or Printer. The Operator typically monitors the status of the Printer and manages and controls the Jobs at the Output Device [RFC2567]. The Operator is allowed to query and control the Printer, Jobs, and Documents based on site policy.

Output Device: A single Logical or Physical Device [STD92].

Personal Data: Information related to a person that can be used to identify the person such as a name, email address, government-issued identification, medical information, and so forth. [IPPPRIVACY]

Physical Device: A hardware implementation of a endpoint device, e.g., a marking engine, a fax modem, etc. [STD92].

Printer Generated Metadata: All Job and Document Status attributes generated by the Printer.

Sensitive Data: Personal Data or other metadata that can be used to correlate or identify a Client or End User.

2.3 Protocol Role Terminology

The following protocol roles are defined to specify unambiguous conformance requirements:

Client: Initiator of outgoing connections and sender of outgoing operation requests (Hypertext Transfer Protocol -- HTTP/1.1 [RFC7230] User Agent).

Printer: Listener for incoming connections and receiver of incoming operation requests (Hypertext Transfer Protocol -- HTTP/1.1 [RFC7230] Server) that represents one or more Physical Devices or a Logical Device.

2.4 Acronyms and Organizations

HTTP: Hypertext Transfer Protocol [RFC7230]

IANA: Internet Assigned Numbers Authority, https://www.iana.org/

IETF: Internet Engineering Task Force, https://www.ietf.org/

ISO: International Organization for Standardization, https://www.iso.org/

NAT: Network Address Translation

PWG: Printer Working Group, https://www.pwg.org/

UI: User Interface

3. Rationale

3.1 Use Cases

3.1.1 Audit Print Usage

Jane manages a shared office multifunction device and wants to know who prints, what kinds of Jobs are printed, how those Jobs are submitted, and where are they printed. She configures a Job Accounting service on her network for use with the Printer so that all Job and Printer Generated Metadata is available to the service and she can then generate reports showing the information she is interested in.

3.1.2 Audit Print Content

Bob is concerned that the students in his computer lab are printing inappropriate content on the school's color printer. He configures a server on his network to act as a print server that stores copies of every Job so that he can periodically review what is being printed.

3.1.3 Billing

Kate is the owner of a managed print service company that supplies printers and print servers to businesses. She collects information about each Job that is printed including whether the Job is printed in color, how many sheets are printed, how many sides are printed, and what finishing options (if any) are used. She uses the collected information to bill each business for their usage and to plan customer visits to perform maintenance or supply additional media, ink, and/or toner based on their usage.

3.1.4 Diagnosing and Debugging Printing Issues

Joe is a support technician at Kate's managed print service company. He uses the accounting data to reproduce problems specific to a particular Document, Job, or Client application.

3.1.5 Supplying Required Information

Some of Kate's larger customers need to be able to track their printing expenses based on their own contract numbers. Kate configures the print server to require the Client to supply a user ID and contract number with every new Job, and then includes the user ID and contract number in the billing reports sent to those customers. Clients will then show the explicit consent UI whenever an End User submits a print Job.

3.1.6 Supplying Optional Information

Some of Kate's customers want to know what applications their End Users are printing from. Kate configures the printer server to request the application name from the Client with every Job, and then includes a separate informational report to her customers showing the amount

of printing that has occurred for each application. Clients will then show the explicit consent UI whenever an End User submits a print Job.

3.1.7 Authenticating End Users

Bob uses authentication to both identify and authorize End Users that submit print Jobs.

3.1.8 Authenticating Print Services

Bob configures his Client computers to require the print services they communicate with to have an X.509 certificate using their company root certificate.

3.1.9 Reconfiguring a Print Service

One of Kate's customers wants to change the information that is tracked for printing. After Kate makes the configuration changes, each Client computer detects the changes and shows the explicit consent UI the next time an End User submits a print Job.

3.2 Exceptions

In addition to the exceptions in the following sub-sections, the standard Internet Printing Protocol/1.1 [STD92] access control, authorization, and role exceptions apply to the use cases defined in section 3.1.

3.2.1 Opt-Out of Mandatory Data Collection

Mary selects a Printer in her Client application for a report she is printing. Her Client application queries the Printer and presents a dialog showing the mandatory data that is required to submit a Job to this Printer. She decides she does not want to send that data and cancels the print request for that Printer. The Client application does not submit a Job to the Printer.

3.2.2 Opt-Out of Optional Data Collection

John selects a Printer in his Client application for a report he is printing. His Client application queries the Printer and presents a dialog showing the optional data that is requested when submitting a Job to this Printer. He decides he does not want to send that data and indicates his preference using the supplied UI before activating the print action. The Client application submits the Job to the Printer without the requested data.

3.3 Out of Scope

The following are considered out of scope for this document:

1. Definition of authentication methods and requirements;
2. Definition of data collection methods outside of IPP;
3. Definition of user account configuration and requirements;
4. Definition of new IPP attributes, values, or operations; and
5. Definition of TLS security requirements.

3.4 Design Requirements

The design requirements for this document are:

1. Define requirements for the authentication of the Client, Printer, and/or End User;
2. Define best practices for the collection of (potentially required) Metadata from the Client;
3. Define best practices for the generation of Metadata by the Printer;
4. Define requirements for explicit privacy and data collection policies that are accessible to/discoverable by Client;
5. Define requirements for explicit consent for all Metadata that is sent from the Client to the Printer;
6. Define best practices for audit logging;
7. Define requirements for data protection;
8. Define best practices for the validation of all Metadata; and
9. Define best practices for interoperability.

4. IPP Model for Job Accounting

IPP provides a rich data model that can be used for Job Accounting. Some Metadata is supplied by the Client while other Metadata is generated by the Printer during Job creation or processing. The following sections describe this Metadata, how a Printer requests or requires specific Metadata, how a Client is expected to obtain explicit consent from the End User, and how a Printer is expected to describe and follow local privacy and data protection policies.

The IPP Model for Job Accounting is based on the following key principles:

> *Accuracy*: All parties will supply and/or generate accurate Metadata that can be validated in various ways;
>
> *Confidentiality*: All parties make best efforts to preserve the confidentiality of Sensitive Data;
>
> *Consent*: The Client obtains explicit consent from the End User to send Sensitive Data to the Printer, and the Printer is configured with a consent policy to accept and process Jobs from authorized End Users; and
>
> *Trust*: All parties establish trust using standards and protocols.

This model works for direct printing from a Client to a Printer representing a Physical Device, printing through local or Cloud-based print servers (Printers representing Logical Devices) where the print server is responsible for collecting and managing Metadata on behalf of the Output Devices, and/or administrative applications that query Printers to provide Job Accounting.

4.1 Client Supplied Metadata

Clients supply attributes in Job or Document Creation requests to specify both print intent and associated Metadata, including the Job name ("job-name") and Document name ("document-name").

Two additional Job Template attributes, "job-accounting-user-id" and "job-account-id" [PWG5100.7], can be supplied to specify End User and billing identifiers for the Job Accounting system separate from the most authenticated user. While these values are not authenticated, they can often be validated against the most authenticated user. These attributes are sometimes used together to specify a logical user for a given organizational account.

Every Client connection to the Printer also carries the Client's network address which can be used by the Printer for access control, logging, and/or recorded as part of the Job Metadata. The validity of the Client network address depends on the network architecture,

proximity of the Client to the Printer, and so forth. In particular, the use of HTTP proxies and NAT can disguise the true source address.

4.2 Printer Generated Metadata

Printers generate attributes and values for Job and Document objects based on the processing they perform. Per the Internet Printing Protocol/1.1 [STD92], the "job-originating-user-name" and "job-originating-user-uri" Job Status attributes contain the most authenticated identity of the Job owner and the "date-time-at-completed (dateTime)", "date-time-at-creation (dateTime)", "date-time-at-processing (dateTime)", "time-at-completed (integer)", "time-at-creation (integer)", and "time-at-processing (integer)" Job Status attributes contain temporal information about the Job.

The "job-impressions", "job-impressions-col", "job-k-octets", "job-media-sheets", "job-media-sheets-col", "job-pages", and "job-pages-col" attributes can be provided by a Client in a Job Creation request but are best generated by the Printer after inspection of the Document data. Similarly, the "impressions", "impressions-col", "k-octets", "media-sheets", "media-sheets-col", "pages", and "pages-col" attributes can be provided by a Client in a Document Creation request but are best generated by the Printer after inspection of the Document data.

Printers provide a receipt of values use for each Job and Document Template attribute in the corresponding "xxx-actual" Job and Document Status attributes. For example, the actual media used for a Job is reported in the "media-col-actual" Job Status attribute.

4.3 Job Creation Requests and Recommended/Required Attributes

The "printer-mandatory-job-attributes (1setOf keyword)" Printer Description attribute [PWG5100.16] is used by a Printer to list the operation and Job Template attributes that a Client needs to supply in a Job Creation Request.

The "printer-requested-job-attributes (1setOf keyword)" Printer Description attribute [PWG5100.16] is used by a Printer to list the operation and Job Template attributes that it would like a Client to supply in a Job Creation Request.

These attributes are typically configured by an Administrator, either using the Set-Printer-Attributes [RFC3380] operation or some out-of-band mechanism.

4.4 Explicit Consent

In any Job Accounting system, certain information is necessary, such as a billing account number, while other information is "nice to have", such as the Client's operating system name and version. Clients following the guidance in this document provide End Users with the ability to control whether necessary and "nice to have" attributes that are not associated

with other UI controls (authenticated user, media settings, etc.) are provided in Job Creation requests. Figure 1 shows one possible UI.

Note: This document does not define a mechanism for the Client to prove to the Printer that the End User has provided explicit consent - if the Client sends the data, the Printer assumes that consent was given. If the End User does not provide explicit consent, a Client following the guidance in this document does not send disallowed Metadata to the Printer.

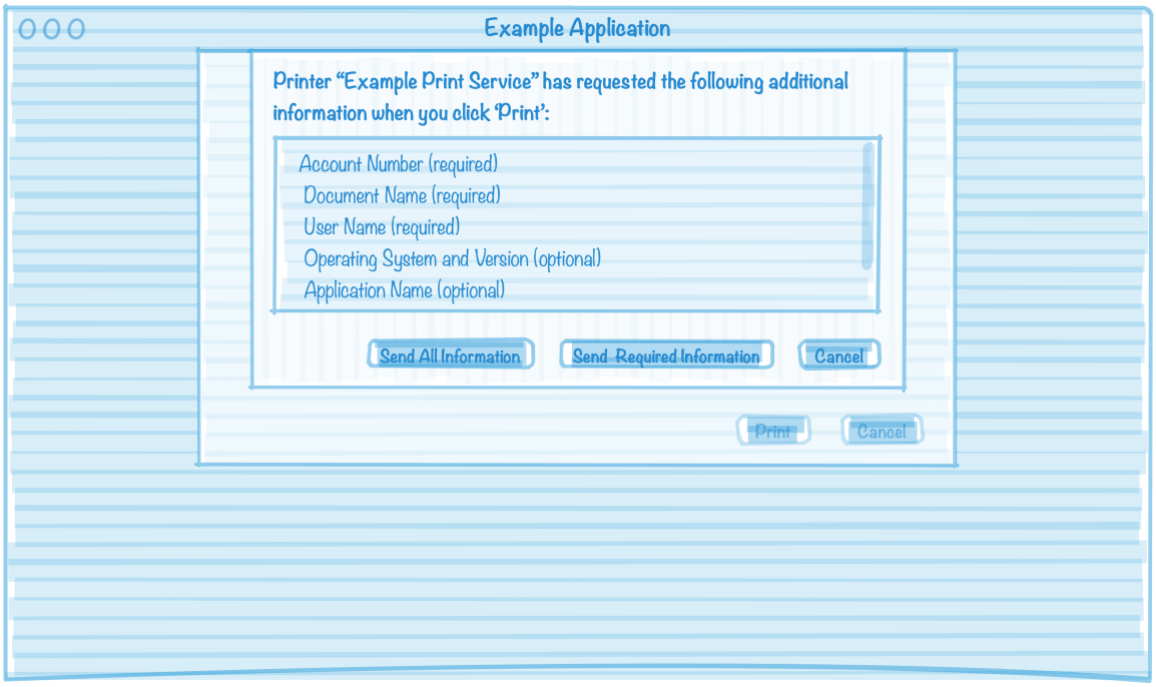

Figure 1 - Example Explicit Consent Dialog

4.5 Privacy and Data Retention Policies

The IPP Privacy Attributes [IPP-PRIVACY] provide a method for a Printer to report its privacy and data retention policies to the Client, which can then be presented to the End User. Printers and Clients following the guidance in this document also conform to the IPP Privacy Attributes.

The IPP Privacy Attributes also enable the Client to discover which Job and Document attributes will be hidden in responses to Get-Jobs and Get-Job-Attributes [STD92] requests.

4.6 Data Validation

One of the key elements of a Job Accounting solution is the validity and accuracy of the accounting data. Typically, Printers can generate accurate Metadata (page counts, dates and times, and so forth) but have limited ability to validate Client-supplied Metadata. Printers can authenticate Client requests and validate Client-supplied Metadata using the most

authenticated End User identity. Printers can reject attributes or values in a Job Creation or Document Creation request by returning the client-error-attributes-or-values-not-supported status code in the response or by adding the corresponding "job-state-reasons" keyword during Job processing.

For example, a Printer could validate the "job-account-id" and "job-accounting-user-id" Job Template attributes by looking up the allowed values for the authenticated End User. Other methods of remote validation are being explored [IETF-RATS] [ITU-X.1254].

4.7 Authenticated Guests

Authenticated Guests allow the Printer to perform ad-hoc validation of the End User. Guest End Users typically provide their name, email address, and/or cellular phone number to create a temporary guest account and are often authenticated using one-time passcodes that are either emailed or delivered via SMS text message to the End User. Once authenticated, the End User identity is stored in the "job-originating-user-name" Job Status attribute [STD92] and potentially the "job-originating-user-uri" Job Status attribute [PWG5100.13] of any submitted Jobs, just as for a non-guest End User.

When using OAuth 2.0 [RFC6749] authentication, the "oauth-authorization-server-uri" Printer Description attribute [PWG5100.18] defines an authorization web page that the Client uses to present the UI to the End User. After entering their identification information, the authorization server sends the passcode to the End User. The End User then enters the passcode to complete the OAuth authorization, allowing the Client to obtain an OAuth 2.0 Bearer Token [RFC6750] to use for authentication of subsequent requests at the HTTP level. This kind of authentication can be discovered by the Client via a Get-Printer-Attributes [STD92] request and presented automatically as needed.

When using HTTP Basic [RFC7617] authentication, the End User first registers with the Printer or when connecting to the network, such as with a Wi-Fi captive portal page. This registration creates a temporary guest account and password that can be used to authenticate subsequent IPP requests.

5. Internationalization Considerations

For interoperability and basic support for multiple languages, conforming implementations support:

1. The Universal Character Set (UCS) Transformation Format -- 8 bit (UTF-8) [STD63] encoding of Unicode [UNICODE] [ISO10646]; and
2. The Unicode Format for Network Interchange [RFC5198] which requires transmission of well-formed UTF-8 strings and recommends transmission of normalized UTF-8 strings in Normalization Form C (NFC) [UAX15].

Unicode NFC is defined as the result of performing Canonical Decomposition (into base characters and combining marks) followed by Canonical Composition (into canonical composed characters wherever Unicode has assigned them).

6. Security Considerations

Job Accounting, as defined in this document, requires the same security considerations as defined in the Internet Printing Protocol/1.1 [STD92], including the TLS considerations in the Opportunistic Security: Some Protection Most of the Time [RFC7435] and Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) [RFC7525]. The following subsections provide considerations specific to this document.

6.1 Client Considerations

Clients MUST:

1. Allow the End User to examine a Printer's privacy and data handling policies;
2. Allow the End User to opt out of sending requested attributes in Job or Document Creation requests;
3. Allow the End User to cancel a Job submission if the End User does not wish to supply mandatory attributes in Job or Document Creation requests;
4. Provide confidentiality of data in transit using TLS encryption [RFC8446] of Printer connections;
5. Authenticate their connections to Printers, such as by validating the Printer's X.509 certificate or using other in-band mutual authentication protocols; and
6. Support authentication of End Users using HTTP authentication methods [PWG5199.10].

6.2 Printer Considerations

Printers MUST:

1. Provide information on configured privacy and data handling policies;
2. Provide lists of optional (requested) and mandatory attributes for Job and Document Creation requests;
3. Validate the HTTP Host request header in order to protect against DNS rebinding attacks;
4. Provide confidentiality of data in transit using TLS encryption [RFC8446] of Client connections;
5. Support authentication of Clients using X.509 certificate validation, HTTP authentication methods, and/or other mechanisms;
6. Support authentication of End Users using HTTP authentication methods [PWG5199.10]; and
7. Provide confidentiality of Document and Job data at rest.

Printers SHOULD support the IPP "-actuals" attributes [PWG5100.8] to provide a Job Receipt for completed Jobs.

6.3 Privacy and Data Collection

Printers SHOULD consider all Job and Document attributes as potentially containing Personal Data. The following attributes explicitly contain Personal Data:

"document-metadata": Contains author information

"job-originating-user-name" and "job-originating-user-uri": The most authenticated Job owner

The following attributes/Metadata can be used to identify individuals or Client devices:

Client Network Address: Provides the Client's source network address, which often identifies the Client device uniquely

"document-format-details": Contains application and operating system information

As a general rule, Personal Data SHOULD be collected and retained only as necessary and discarded when it is no longer needed.

6.4 Data Protection

Printers MUST protect Job and Document data in transit using TLS encryption [RFC8446]. Printers SHOULD protect Job and Document data at rest using encrypted storage and available secure access controls and containment features provided by the Printer's operating system software.

6.5 Data Validation

Printers SHOULD validate all attributes, values, and Document data that are submitted by a Client.

Printers SHOULD also authenticate all Job and Document Creation requests so that the identity of the End User can be validated.

Printers that do billing and allow guest printing SHOULD implement Authenticated Guest printing (section 4.7) to allow for validation of the guest's identity for proper billing.

7. Common Job Accounting Metadata

Table 1 lists the IPP attributes commonly used for Job Accounting. The full list of Job Description, Job Status, and Job Template attributes can be found in the IANA IPP Registry [IANA-IPP].

Table 1 - Common Job Accounting Metadata

Attribute	Description	Source
copies (integer(1:MAX))	Number of copies	Client
date-time-at-completed (dateTime | no-value)	Date/time when completed	Printer
date-time-at-creation (dateTime)	Date/time when created	Printer
date-time-at-processing (dateTime | no-value)	Date/time when printed	Printer
document-format (mimeMediaType)	Format of document	Client
document-format-details (collection)	Application/OS name/version	Client
document-name (name(MAX))	Document name	Client
document-uuid (uri(45))	Document UUID	Printer
finishings (1setOf type2 enum) finishings-col (1setOf collection)	Finisher options (staple, punch, etc.)	Client
job-account-id (name(MAX))	Accounting identifier	Client
job-account-type (type2 keyword | name(MAX))	Identifer type	Client
job-accounting-user-id (name(MAX))	Accounting user ID	Client
job-id (integer(1:MAX))	Job ID	Printer
job-impressions (integer(0:MAX)) job-impressions-col (collection)	Number of sides	Printer
job-impressions-completed (integer(0:MAX)) job-impressions-completed-col (collection)	Number of sides printed	Printer
job-media-sheets (integer(0:MAX)) job-media-sheets-col (collection)	Number of sheets	Printer
job-media-sheets-completed (integer(0:MAX)) job-media-sheets-completed-col (collection)	Number of sheets printed	Printer
job-name (name(MAX))	Job name/title	Client
job-originating-user-name (name(MAX))	End User name	Client
job-originating-user-uri (uri)	End User URI	Client
job-pages (integer(0:MAX)) job-pages-col (collection)	Number of pages	Printer
job-pages-completed (integer(0:MAX)) job-pages-completed-col (collection)	Number of pages printed	Printer
job-priority (integer(0:100))	Job priority	Client
job-printer-uri (uri)	Printer	Printer
job-state (type1 enum)	Job state	Printer
job-state-reasons (1setOf type2 keyword)	Detailed job state	Printer
job-uuid (uri)	Job UUID	Printer
media (type2 keyword | name(MAX)) media-col (collection)	Media to use	Client
print-color-mode (type2 keyword)	Color/B&W print mode	Client
print-quality (type2 enum)	Print quality (draft/normal/high)	Client
printer-resolution (resolution)	Print resolution	Client
sides (type2 keyword)	Duplex mode	Client
time-at-completed (integer(0:MAX) | no-value)	Relative time when completed	Printer
time-at-creation (integer(0:MAX))	Relative time when created	Printer
time-at-processing (integer(0:MAX) | no-value)	Relative time when printed	Printer

8. References

[BCP14] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119/BCP 14, March 1997, https://tools.ietf.org/html/bcp14

[IANA-IPP] "IANA IPP Registry", https://www.iana.org/assignments/ipp-registrations/ipp-registrations.xml

[IETF-RATS] "IETF Remote Attestation Procedures Workgroup", https://tools.ietf.org/wg/rats/

[IPPPRIVACY] M. Sweet, "IPP Privacy Attributes v1.0 (PRIVACY)", IPP Registration, April 18, 2018, https://ftp.pwg.org/pub/pwg/ipp/registrations/reg-ippprivacy10-20180412.pdf

[ISO10646] "Information technology -- Universal Coded Character Set (UCS)", ISO/IEC 10646:2014

[ITU-X.1254] "Entity authentication assurance framework", Recommendation ITU-T X.1254, September 2020, https://www.itu.int/

[PWG5100.7] M. Sweet, "IPP Job Extensions v2.0 (JOBEXT)", PWG 5100.7-2019, August 2019, https://ftp.pwg.org/pub/pwg/candidates/cs-ippjobext20-20190816-5100.7.pdf

[PWG5100.8] "Standard for Internet Printing Protocol (IPP): '-actuals' attributes", PWG 5100.8-2003, March 2003, https://ftp.pwg.org/pub/pwg/candidates/cs-ippactuals10-20030313-5100.8.pdf

[PWG5100.13] M. Sweet, I. McDonald, P. Zehler, "IPP Job and Printer Extensions - Set 3 (JPS3)", PWG 5100.13-2012, July 2012, https://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext3v10-20120727-5100.13.pdf

[PWG5100.16] M. Sweet, "IPP Transaction-Based Printing Extensions v1.1 (TRANS)", PWG 5100.16-2020, March 2020, https://ftp.pwg.org/pub/pwg/candidates/cs-ipptrans11-20200327-5100.16.pdf

[PWG5100.18] M. Sweet, "IPP Shared Infrastructure Extensions (INFRA)", PWG 5100.18-2015, June 2015, https://ftp.pwg.org/pub/pwg/candidates/cs-ippinfra10-20150619-5100.18.pdf

[PWG5199.10] S. Kennedy, "IPP Authentication Methods v1.0", PWG 5199.10-2019, https://ftp.pwg.org/pub/pwg/informational/bp-ippauth10-20190816-5199.10.pdf

[RFC2567] F.D. Wright, "Design Goals for an Internet Printing Protocol", RFC 2567, April 1999, https://tools.ietf.org/html/rfc2567

[RFC3380] T. Hastings, R. Herriot, C. Kugler, H. Lewis, "Internet Printing Protocol (IPP): Job and Printer Set Operations", RFC 3380, September 2002, https://tools.ietf.org/html/rfc3380

[RFC5198] J. Klensin, M. Padlipsky, "Unicode Format for Network Interchange", RFC 5198, March 2008, https://tools.ietf.org/html/rfc5198

[RFC6749] D. Hardt, "The OAuth 2.0 Authorization Framework", RFC 6749, October 2012, https://tools.ietf.org/html/rfc6749

[RFC6750] M. Jones, D. Hardt, "The OAuth 2.0 Authorization Framework: Bearer Token Usage", RFC 6750, October 2012, https://tools.ietf.org/html/rfc6750

[RFC7230] R. Fielding, J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, June 2014, https://tools.ietf.org/html/rfc7230

[RFC7435] V. Dukhovni, "Opportunistic Security: Some Protection Most of the Time", RFC 7435, December 2014, https://tools.ietf.org/html/rfc7435

[RFC7525] Y. Sheffer, R. Holz, P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", RFC 7525, May 2015, https://tools.ietf.org/html/rfc7525

[RFC7617] J. Reschke, "The 'Basic' Authentication Scheme", RFC 7617, September 2015, https://tools.ietf.org/html/rfc7617

[RFC8446] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, August 2018, https://tools.ietf.org/html/rfc8446

[STD63] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC 3629/STD 63, November 2003, https://tools.ietf.org/html/std63

[STD92] M. Sweet, I. McDonald, "Internet Printing Protocol/1.1", STD 92, June 2018, https://tools.ietf.org/html/std92

[UAX15] M. Davis, M. Duerst, "Unicode Normalization Forms", Unicode Standard Annex 15, May 2018, https://www.unicode.org/reports/tr15

[UNICODE] Unicode Consortium, "Unicode Standard", Version 13.0.0, March 2020, https://www.unicode.org/versions/Unicode13.0.0/

9. Author's Address

Primary author:

Michael Sweet
Lakeside Robotics Corporation

The author would also like to thank the following individuals for their contributions to this best practice:

Cihan Colakoglu - Kyocera
Smith Kennedy - HP Inc.
Ira McDonald - High North
Jeremy Reitz - Xerox

