Job Accounting with IPP v1.0

Status: Interim

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:


This best practice is available electronically at:


Copyright © 2019 2020 The Printer Working Group. All rights reserved.
Copyright © 2019-2020 The Printer Working Group. All rights reserved.

Title: Job Accounting with IPP v1.0

The material contained herein is not a license, either expressed or implied, to any IPR owned or controlled by any of the authors or developers of this material or the Printer Working Group. The material contained herein is provided on an “AS IS” basis and to the maximum extent permitted by applicable law, this material is provided AS IS AND WITH ALL FAULTS, and the authors and developers of this material and the Printer Working Group and its members hereby disclaim all warranties and conditions, either expressed, implied or statutory, including, but not limited to, any (if any) implied warranties that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.
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 ....................................... 6
3. Rationale ................................................................. 8
  3.1 Use Cases ............................................................... 8
  3.1.1 Auditing of Printing Usage ...................................... 8
  3.1.2 Auditing of Print Content ....................................... 8
  3.1.3 Billing ................................................................. 8
  3.1.4 Diagnostics and Debugging ..................................... 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
4. Job Accounting with IPP ................................................ 10
  4.1 Client Supplied Metadata .......................................... 10
  4.2 Printer Generated Metadata ....................................... 10
  4.3 Job Creation Requests and Recommended/Required Attributes 11
  4.4 Explicit Consent ...................................................... 11
  4.5 Privacy and Data Retention Policies .............................. 12
5. New Attributes .......................................................... 12
  5.1 Printer Description Attributes ..................................... 12
  5.1.1 printer-requested-job-attributes (1setOf keyword) ........... 12
6. Internationalization Considerations ................................ 13
7. Security Considerations ................................................. 13
  7.1 Client Considerations .............................................. 13
  7.2 Printer Considerations ............................................. 14
  7.3 Privacy and Data Collection ..................................... 14
  7.4 Data Protection ....................................................... 14
  7.5 Data Validation ...................................................... 14
8. References ....................................................................... 15
9. Author's Address .......................................................... 16
10. Change History ................................................................ 17
  10.1 January 29, 2020 ...................................................... 17
  10.2 October 22, 2019 ..................................................... 17
  10.3 April 18, 2019 ......................................................... 18
List of Figures

Figure 1 - Example Explicit Consent Dialog.................................................................12
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].

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.

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.
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.

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

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 an endpoint device, e.g., a marking engine, a fax modem, etc.

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

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

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


UI: User Interface
3. Rationale

3.1 Use Cases

3.1.1 Auditing of Printing Usage
Jane manages a shared office multifunction device and wants to know who prints, what kinds of Jobs are printed, how are 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 Jobs are routed through the service and she can then generate reports showing the information she is interested in.

3.1.2 Auditing of 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 on, how many sides are printed on, 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 Diagnostics and Debugging
Joe is a support technician at Kate’s managed print service company. He uses the accounting data to reproduce problems specific to a particular 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.

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.
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 she 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 3.2.

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 user account configuration and requirements; and
3. 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

4. Job Accounting with IPP

4.1 Client Supplied Metadata

Clients supply attributes in Job or Document Creation requests to specify both print intent and informational 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 authenticated user. While these values are not authenticated, they can often be validated against the authenticated user. These attributes are sometimes used together to specify a logical user for a given organizational account.

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.

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 [PWG5100.13] is used by a Printer to list the operation and Job Template attributes that a Client MUST supply in a Job Creation Request. Clients MUST support this attribute and Printers MUST supply this attribute if specific attributes are needed for Job Accounting.

The "printer-requested-job-attributes (1setOf keyword)" Printer Description attribute (section 5.1.1) is used by a Printer to list the operation and Job Template attributes that a Client SHOULD supply in a Job Creation Request. Clients SHOULD support this attribute and Printers MUST supply this attribute if specific attributes are used but not required for Job Accounting.

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 MUST 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.
4.5 Privacy and Data Retention Policies

The IPP Privacy Attributes [IPP-PRIVACY] provide a framework 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 conforming to this document MUST also conform to the IPP Privacy Attributes.

5. New Attributes

5.1 Printer Description Attributes

5.1.1 printer-requested-job-attributes (1setOf keyword)

This RECOMMENDED attribute lists the attributes the Printer wants but does not need in order to support Job Accounting. Member attributes of collections are specified by concatenating attribute names delimited by the period (".") character, e.g., the "document-source-application-name" member attribute of the "document-format-details" operation attribute [PWG5100.7] would be requested using the keyword value 'document-format-details.document-source-application-name'. If supported, Clients MUST allow the End User to explicitly consent to the sending of any attributes or values that are not explicitly chosen by the End User.
For example, a Printer can list the 'media' and 'media-col keywords in "printer-requested-
job-attributes". If the Client application provides a UI control for selecting a media size, no
additional consent is needed since the UI allows the User to select which value is sent.

However, if a Printer lists the "document-format-details.document-source-application-name"
keyword in "printer-requested-job-attributes", it is unlikely that the Client application will
provide a UI control for selecting the application name that is sent to the Printer. In this case,
the Client MUST provide a UI that allows the End User to opt out of sending the requested
information. If the End User opts out of sending the requested information, the Client MUST
NOT send it.

6. 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).

7. Security Considerations

The IPP extensions defined in this document require the same security considerations as
declared 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.

7.1 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;

Page 13 of 18  Copyright © 2019-2020 The Printer Working Group. All rights reserved.
4. Provide confidentiality of data in transit using TLS encryption [RFC5246] 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

7.2 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;
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; and
7. Provide confidentiality of Document and Job data at rest.

7.3 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 can be used to identify individuals or Client devices:

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

7.4 Data Protection

TBD

7.5 Data Validation

TPM mechanisms to provide signed information?
Using Client/Printer/User authentication as a source of trust?
8. References


9. Author’s Address

Primary author:

Michael Sweet
Apple Inc.
One Apple Park Way
M/S 111-HOMC
Cupertino, CA 95014
USA
msweet@apple.com

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

Cihan Colakoglu - Kyocera
Smith Kennedy - Hewlett Packard
Ira McDonald - High North
Jeremy Reitz - Xerox
10. Change History

10.1 January 29, 2020

- Added discussion of user and printer authentication in use cases
- Added discussion of changing consent requirements in new use case
- Section 3.1.5: Added user ID
- Section 3.3: Added definition of user account configuration/requirements
- Section 4.3: Updated title, added reference to RFC 3380
- Global: Use "explicit consent" throughout
- Section 4.4: Clarify that only information not entered through UI controls needs explicit consent
- Sections 7 and 8: Added references to RFC 7435 and 7525
- Section 8: Add reference to RFC 3380

10.2 October 22, 2019

- Status: Interim
- Section 2: Added some terms and acronyms that were missing.
- Section 3: Cleaned up use cases, out of scope, and design requirements.
- Section 3.2: Added exceptions.
- Section 4: Added discussion of informed consent, notion of required and requested attributes/values for accounting.
- New Section 5: "printer-requested-job-attributes"
- Section 7.1: Added explicit informed consent
- Section 7.2: Added printer-requested-job-attributes
- Updated references.
10.3 April 18, 2019

Initial revision.