The Printer Working Group

April 12, 2018
IPP Registration

IPP Privacy Attributes v1.0 (PRIVACY)

Status: IPP Workgroup Approved

Abstract: This registration defines attributes for specifying the privacy policies of Document, Job, Printer, and Subscription objects.

This registration is available electronically at:

https://ftp.pwg.org/pub/pwg/ipp/registrations/reg-ippprivacy10-20180412.docx
https://ftp.pwg.org/pub/pwg/ipp/registrations/reg-ippprivacy10-20180412.pdf

Title: *IPP Privacy Attributes v1.0 (PRIVACY)*

Table of Contents

1. Introduction

Many political regions require explicit or implied consent when processing Personal and Confidential Data, such as the European Union's General Data Protection Regulation [GDPR]. While the Internet Printing Protocol/1.1: Model and Semantics [RFC8011] defines general access rights and privacy policies for Printers and associated objects, it does not define a way for Clients to discover what the specific access rights and policies are for a given Printer.

This registration defines Printer Description attributes that specify the privacy policies of Document, Job, Printer, and Subscription object attributes. The attributes are based on the privacy controls provided by the CUPS printing system [CUPS] and allow a Client to determine which attributes are considered private and which End Users will be able to access them. The privacy attributes are potentially configurable by an authorized Administrator using the Set-Printer-Attributes operation [RFC3998].

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.

2.2 Printing Terminology

Normative definitions and semantics of printing terms are imported from IETF Printer MIB v2 [RFC3805], IETF Finisher MIB [RFC3806], and IETF Internet Printing Protocol/1.1: Model and Semantics [RFC8011].

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].

Confidential Data: Information that should not be made publicly available, including legal documents, financial information, Personal Data, and organizational data.

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.

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.

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.

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

Subscription: An object created and managed by a Printer that contains description, event, and status information. Subscriptions monitor for state and configuration changes to Jobs and Printers.

2.3 Protocol Role Terminology

This document also defines the following protocol roles 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/

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

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

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

3. Requirements

3.1 Rationale

The Internet Printing Protocol/1.1: Model and Semantics [RFC8011] defines general access rights and privacy policies for Printers and associated objects but does not define a way for Clients to discover what the specific rights and policies are for a given Printer.

Given that many countries require explicit or implied consent when processing Personal and Confidential Data, this registration should:

1. Define attributes describing which Document, Job, and Subscription object attributes are subject to privacy controls,
2. Define attributes describing which End Users may access attributes subject to privacy controls,
3. Define an attribute referencing the Printer's written privacy policy, and
4. Define security considerations for the configuration and use of the privacy attributes.

3.2 Use Cases

3.2.1 Limit Access to Sensitive Information

Jane submits a Job for printing that contains confidential information about her company to a shared printer in the office. Since the Job does contain confidential information, she would like the Job attributes to be hidden from other employees of the company.

3.3 Out of Scope

The following are considered out of scope for this registration:

1. Definition of new file formats; and
2. Definition of new protocol bindings.

3.4 Design Requirements

The design requirements for this registration are:

1. Define attributes and values to describe the privacy policy of the Printer; and
2. Define sections to register all attributes and values with IANA.

4. New Attributes

4.1 Printer Description Attributes

4.1.1 document-privacy-attributes (1setOf type2 keyword)

This CONDITIONALLY REQUIRED attribute specifies which Document object attributes are considered private. Printers that support the Document object MUST support this attribute. In addition to attribute names, the following keyword values are defined:

'all': All attributes except "document-job-id", "document-job-uri", "document-number", "document-printer-uri", and "document-uuid" are private.

'default': All Document Description and Template attributes are private.

'document-description': All Document Description attributes are private.

'document-template': All Document Template attributes are private.

'none': No attributes are private.

If the 'none' value is specified, it MUST be the only value.

4.1.2 document-privacy-scope (type2 keyword)

This CONDITIONALLY REQUIRED attribute specifies which End Users are allowed to query private Document object attributes using the Get-Documents and Get-Document-Attributes operations. Printers that support the Document object MUST support this attribute. The following keyword values are defined (ordered from most permissive to least permissive):

'all': All End Users have access to private attributes.

'default': The Document owner and any Operator or Administrator has access to private attributes.

'owner': Only the Document owner has access to private attributes.

'none': No End User has access to private attributes.

4.1.3 job-privacy-attributes (1setOf type2 keyword)

This REQUIRED attribute specifies which Job object attributes are considered private. In addition to attribute names, the following keyword values are defined:

'all': All attributes except "job-id", "job-uri", "job-uuid", and "job-printer-uri" are private.

'default': All Job Description and Template attributes are private.

'job-description: All Job Description attributes are private.

'job-template': All Job Template attributes are private.

'none': No attributes are private.

If the 'none' value is specified, it MUST be the only value.

4.1.4 job-privacy-scope (type2 keyword)

This REQUIRED attribute specifies which End Users are allowed to query private Job object attributes using the Get-Jobs and Get-Job-Attributes operations. The following keyword values are defined (from most permissive to least permissive):

'all': All End Users have access to private attributes.

'default': The Job owner and any Operator or Administrator has access to private attributes.

'owner': Only the Job owner has access to private attributes.

'none': No End User has access to private attributes.

4.1.5 printer-privacy-policy-uri (uri)

This REQUIRED attribute specifies the URI for the Printer's written privacy policy, typically as a page that can be viewed in an embedded web view or browser application. The privacy policy typically addresses:

1. What Personal and/or Confidential Data might be collected by the Printer;
2. How the Personal and Confidential Data is used by the Printer;
3. How the Personal and Confidential Data is stored on the Printer;
4. How access to the Personal and Confidential Data is protected by the Printer; and
5. Whether the Personal and Confidential Data is transferred off the Printer.

4.1.6 subscription-privacy-attributes (1setOf type2 keyword)

This CONDITIONALLY REQUIRED attribute specifies which Subscription object attributes are considered private. Printers that support the Subscription object MUST support this attribute. In addition to attribute names, the following keyword values are defined:

'all': All attributes except "notify-job-id", "notify-printer-uri", "notify-subscription-id", and "notify-subscription-uuid" are private.

'default': All Subscription Description and Template attributes are private.

'subscription-description: All Subscription Description attributes are private.

'subscription-template': All Subscription Template attributes are private.

'none': No attributes are private.

If the 'none' value is specified, it MUST be the only value.

4.1.7 subscription-privacy-scope (type2 keyword)

This CONDITIONALLY REQUIRED attribute specifies which End Users are allowed to query private Subscription object attributes using the Get-Subscriptions and Get-Subscription-Attributes operations. Printers that support the Subscription object MUST support this attribute. The following keyword values are defined (from most permissive to least permissive):

'all': All End Users have access to private attributes.

'default': The Subscription owner and any Operator or Administrator has access to private attributes.

'owner': Only the Subscription owner has access to private attributes.

'none': No End User has access to private attributes.

5. Conformance Requirements

5.1 Printer Conformance Requirements

In order for a Printer to claim conformance to this document, a Printer MUST support:

1. The required attributes and values defined in section 4;
2. The internationalization considerations defined in section 0; and
3. The security considerations defined in section 7.

5.2 Client Conformance Requirements

In order for a Client to claim conformance to this document, a Client MUST support:

1. The required attributes and values defined in section 4;
2. The internationalization considerations defined in section 0; and
3. The security considerations defined in section 7.

6. Internationalization Considerations

For interoperability and basic support for multiple languages, conforming implementations MUST 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).

WARNING – Performing normalization on UTF-8 strings received from Clients and subsequently storing the results (e.g., in Job objects) could cause false negatives in Client searches and failed access (e.g., to Printers with percent-encoded UTF-8 URIs now 'hidden').

Implementations of this specification SHOULD conform to the following standards on processing of human-readable Unicode text strings, see:

Unicode Bidirectional Algorithm [UAX9] – left-to-right, right-to-left, and vertical

Unicode Line Breaking Algorithm [UAX14] – character classes and wrapping

Unicode Normalization Forms [UAX15] – especially NFC for [RFC5198]

Unicode Text Segmentation [UAX29] – grapheme clusters, words, sentences

Unicode Identifier and Pattern Syntax [UAX31] – identifier use and normalization

Unicode Collation Algorithm [UTS10] – sorting

Unicode Locale Data Markup Language [UTS35] – locale databases

Implementations of this specification are advised to also review the following informational documents on processing of human-readable Unicode text strings:

Unicode Character Encoding Model [UTR17] – multi-layer character model

Unicode in XML and other Markup Languages [UTR20] – XML usage

Unicode Character Property Model [UTR23] – character properties

Unicode Conformance Model [UTR33] – Unicode conformance basis

7. Security Considerations

The IPP extensions defined in this document require the same security considerations as defined in the IPP/1.1: Model and Semantics [RFC8011]. The following subsections provide considerations specific to this registration.

7.1 Text Processing

Implementations of this specification SHOULD conform to the following standard on processing of human-readable Unicode text strings:

Unicode Security Mechanisms [UTS39] – detecting and avoiding security attacks

Implementations of this specification are advised to also review the following informational document on processing of human-readable Unicode text strings:

Unicode Security FAQ [UNISECFAQ] – common Unicode security issues

7.2 Access Control and Authorization for Configuration of Privacy Attributes

Printers MAY allow authorized Clients to change the values of the privacy attributes defined in this specification using the Set-Printer-Attributes [RFC3998] operation. Because changing the privacy attributes can have legal implications, Printers MUST only support such operations over a secure channel with sufficient authentication to prevent unauthorized access and configuration. Printers MUST also maintain an audit log of all such changes.

7.3 Protection of Data at Rest

Printers MUST support protection of data at rest, including all Document, Job, and Subscription object attributes and Document data. Protection includes encryption and isolation of the affected data when not in use.

7.4 Logging

Printers MUST support logging of all changes to privacy attributes and SHOULD support logging of all accesses to private attributes of objects under the Printer's control.

8. IANA Considerations

8.1 Attribute Registrations

The attributes defined in this registration will be published by IANA according to the procedures in IPP/1.1 Model and Semantics [RFC8011] section 7.2 in the following file:

http://www.iana.org/assignments/ipp-registrations

The registry entries will contain the following information:

Printer Description attributes:	Reference
document-privacy-attributes (1setOf type2 keyword)	[PRIVACY]
document-privacy-scope (type2 keyword)	[PRIVACY]
job-privacy-attributes (1setOf type2 keyword)	[PRIVACY]
job-privacy-scope (type2 keyword)	[PRIVACY]
printer-privacy-policy-uri (uri)	[PRIVACY]
subscription-privacy-attributes (1setOf type2 keyword)	[PRIVACY]
subscription-privacy-scope (type2 keyword)	[PRIVACY]

8.2 Attribute Value Registrations

The attributes defined in this registration will be published by IANA according to the procedures in IPP/1.1 Model and Semantics [RFC8011] section 7.1 in the following file:

http://www.iana.org/assignments/ipp-registrations

The registry entries will contain the following information:

Attributes (attribute syntax) Keyword Attribute Value	Reference
document-privacy-attributes (1setOf type2 keyword)	[PRIVACY]
< any Document object attribute >	[PRIVACY]
all	[PRIVACY]
default	[PRIVACY]
document-description	[PRIVACY]
document-template	[PRIVACY]
none	[PRIVACY]
document-privacy-scope (type2 keyword)	[PRIVACY]
all	[PRIVACY]
default	[PRIVACY]
none	[PRIVACY]
owner	[PRIVACY]
job-privacy-attributes (1setOf type2 keyword)	[PRIVACY]
< any Job object attribute >	[PRIVACY]
all	[PRIVACY]
default	[PRIVACY]


```
    job-description                                          [PRIVACY]
    job-template                                             [PRIVACY]
    none                                                     [PRIVACY]

  job-privacy-scope (type2 keyword)                          [PRIVACY]
    all                                                      [PRIVACY]
    default                                                  [PRIVACY]
    none                                                     [PRIVACY]
    owner                                                    [PRIVACY]

  subscription-privacy-attributes (1setOf type2 keyword)     [PRIVACY]
    < any Subscription object attribute >                    [PRIVACY]
    all                                                      [PRIVACY]
    default                                                  [PRIVACY]
    subscription-description                                 [PRIVACY]
    subscription-template                                    [PRIVACY]
    none                                                     [PRIVACY]

  subscription-privacy-scope (type2 keyword)                 [PRIVACY]
    all                                                      [PRIVACY]
    default                                                  [PRIVACY]
    none                                                     [PRIVACY]
    owner                                                    [PRIVACY]
```

9. References

9.1 Normative 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/rfc2119

[ISO10646] "Information technology -- Universal Coded Character Set (UCS)", ISO/IEC 10646:2011

[RFC3998] C. Kugler, H. Lewis, T. Hastings, "Internet Printing Protocol (IPP): Job and Printer Administrative Operations", RFC 3998, March 2005, https://tools.ietf.org/html/rfc3998

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

[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

[RFC8011] M. Sweet, I. McDonald, "Internet Printing Protocol/1.1: Model and Semantics", RFC 8011, January 2017, https://tools.ietf.org/html/rfc8011

[STD63] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC 3629/STD 63, November 2003, https://tools.ietf.org/html/rfc3629

[STD66] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", RFC 3986/STD 66, January 2005, https://tools.ietf.org/html/rfc3986

[UAX9] Unicode Consortium, “Unicode Bidirectional Algorithm”, UAX#9, June 2014, https://www.unicode.org/reports/tr9/tr9-31.html

[UAX14] Unicode Consortium, “Unicode Line Breaking Algorithm”, UAX#14, June 2014, https://www.unicode.org/reports/tr14/tr14-33.html

[UAX15] Unicode Consortium, “Normalization Forms”, UAX#15, June 2014, https://www.unicode.org/reports/tr15/tr15-41.html

[UAX29] Unicode Consortium, “Unicode Text Segmentation”, UAX#29, June 2014, https://www.unicode.org/reports/tr29/tr29-25.html

[UAX31] Unicode Consortium, “Unicode Identifier and Pattern Syntax”, UAX#31, June 2014, https://www.unicode.org/reports/tr31/tr31-21.html

[UNICODE] Unicode Consortium, "Unicode Standard", Version 10.0.0, June 2017, https://www.unicode.org/versions/Unicode10.0.0/

[UTS10] Unicode Consortium, “Unicode Collation Algorithm”, UTS#10, June 2014, https://www.unicode.org/reports/tr10/tr10-30.html

[UTS35] Unicode Consortium, “Unicode Locale Data Markup Language”, UTS#35, September 2014, https://www.unicode.org/reports/tr35/tr35-37/tr35.html

[UTS39] Unicode Consortium, “Unicode Security Mechanisms”, UTS#39, September 2014, https://www.unicode.org/reports/tr39/tr39-9.html

9.2 Informative References

[CUPS] "CUPS Project Home Page", https://www.cups.org/

[GDPR] "General Data Protection Regulation", http://eur-lex.europa.eu/eli/reg/2016/679/oj

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

[UTR17] Unicode Consortium “Unicode Character Encoding Model”, UTR#17, November 2008, https://www.unicode.org/reports/tr17/tr17-7.html

[UTR20] Unicode Consortium “Unicode in XML and other Markup Languages”, UTR#20, January 2013, https://www.unicode.org/reports/tr20/tr20-9.html

[UTR23] Unicode Consortium “Unicode Character Property Model”, UTR#23, November 2008, https://www.unicode.org/reports/tr23/tr23-9.html

[UTR33] Unicode Consortium “Unicode Conformance Model”, UTR#33, November 2008, https://www.unicode.org/reports/tr33/tr33-5.html

[UNISECFAQ] Unicode Consortium “Unicode Security FAQ”, November 2013, https://www.unicode.org/faq/security.html

10. Authors' Addresses

Primary authors:

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

