The Printer Working Group

June 4, 2020
IPP Registration

IPP System Service Discovery v1.0

Status: IPP Workgroup Approved

Abstract: This registration defines an IPP attribute and DNS-SD service type to support discovery of IPP System Services (PWG 5100.22).

This registration is available electronically at:

https://ftp.pwg.org/pub/pwg/ipp/registrations/reg-ippsysdisc10-20200604.docx
https://ftp.pwg.org/pub/pwg/ipp/registrations/reg-ippsysdisc10-20200604.pdf

Title: *IPP System Service Discovery v1.0*

Table of Contents

List of Tables

1. Introduction

The IPP System Service v1.0 specification [PWG5100.22] defines an IPP binding of the PWG Semantic Model System Object and System Control Service [PWG5108.06], but does not define a method of discovering systems that implement it. This registration defines an IPP attribute and DNS-SD service type to support discovery of IPP Systems.

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 IETF Printer MIB v2 [RFC3805], IETF Finisher MIB [RFC3806], and IETF Internet Printing Protocol/1.1 [STD92].

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.

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.

Output Device: a single Logical or Physical Device

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

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).

System: Listener for incoming IPP session requests and receiver of incoming IPP operation requests (Hypertext Transfer Protocol -- HTTP/1.1 [RFC7230] Server) that exposes an IPP System object and implements a System Service.

2.4 Acronyms and Organizations

DNS-SD: Domain Name System Based Service Discovery [RFC6763]

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/

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

3. Requirements

3.1 Rationale

Given the following existing specifications:

1. IPP System Service v1.0 (SYSTEM) [PWG5100.22]
2. Multicast DNS [RFC6762]
3. DNS-Based Service Discovery [RFC6763]

And given the need to discover IPP System Services, the IPP System Service Discovery v1.0 registration should:

1. Define attributes needed to support DNS-SD, and
2. Define a DNS-SD service type for IPP System Services.

3.2 Use Cases

3.2.1 Discover an IPP System Service

Jane is managing the printing services on an enterprise network. She uses a management application on her Client device to find the IPP System Services on her network and configure and monitor the various imaging services they provide.

3.3 Exceptions

There are no exceptions beyond those defined in the Internet Printing Protocol/1.1 [STD92].

3.4 Out of Scope

The following are considered out of scope for this registration:

1. Definition of new discovery protocols.

3.5 Design Requirements

The design requirements for this registration are:

1. Define an attribute for the DNS-SD service name;
2. Define a DNS-SD service type for the IPP System Service; and
3. Define sections to register the attribute and service type with IANA.

4. Model

The IPP Everywhere [PWG5100.14] specification defines a mechanism for discovery of IPP Printers. This registration defines an equivalent mechanism with an associated System Description attribute for the advertised service name.

5. Discovery

5.1 DNS-Based Service Discovery

DNS-Based Service Discovery (DNS-SD) [RFC6763] uses service (SRV) records and traditional unicast and multicast DNS (mDNS) [RFC6762] queries. Services are identified by a service instance name consisting of an instance name, a service type or subtype name, and a domain name. Discovery of Systems involves a single service type as described in the following sections.

Systems that support DNS-SD MUST support mDNS and MAY support dynamic DNS updates via Dynamic Updates in the Domain Name System (DNS UPDATE) [RFC2136] and other mechanisms.

5.1.1 IPP System Service Type

This specification defines the "_ipps-system._tcp" service type to allow Clients to discover Systems. Because the IPP System Service v1.0 [PWG5100.22] REQUIRES implementations to support IPPS [RFC7472], there is no non-IPPS service type.

5.1.2 Service (SRV) Instance Name

Systems MUST NOT use a service instance name containing a unique identifier by default. A unique identifier MAY be added to the instance if there is a name collision.

The domain portion of the service instance name MUST BE "local." for mDNS.

Systems that support DNS-SD MUST advertise the "_ipps-system._tcp" service over mDNS. For example, a System named "Example System" would advertise the service instance name "Example System._ipps-system._tcp.local.".

5.1.3 Geo-Location (LOC)

Systems MUST publish LOC records [RFC1876] over mDNS to provide the physical location of the System. Systems MUST allow the End User to configure the geo-location manually. If the accuracy of the geo-location is unknown, a value of 9×10^9 meters (0x99) MUST be used.

5.1.4 Text (TXT)

Systems MUST publish a text (TXT) record that provides service information over mDNS. Systems that support dynamic DNS updates MUST publish separate TXT records for each domain that is updated. Table 1 lists all the key/value pairs that are defined with the corresponding default values. Systems SHOULD omit key/value pairs when the value matches the default value for the corresponding key to limit the size of the TXT record.

The combined length of a TXT key/value pair ("key=value") cannot exceed 255 octets. This limit is sometimes smaller than the limit imposed by the corresponding IPP attribute.

The combined length of all TXT key/value pairs provided by the System SHOULD BE 400 octets or less for unicast DNS and MUST NOT exceed 1300 octets for multicast DNS.

Clients MUST ignore incomplete key/value pairs at the end of a truncated TXT record.

Table 1 - DNS TXT Record Keys

Key	Description	Default Value
air	The type of authentication information that is required for the System as reported by the "system-xri-supported.xri-authentication" attribute values.	'none'
note	The location of the System as reported by the "system-location" System Description attribute.	'' (empty string)
UUID	The UUID of the System without the 'urn:uuid:' prefix as reported by the "system-uuid" System Status attribute.	'' (empty string)

5.1.4.1 air

The "air" key defines the type of authentication information that is required for imaging. The value is derived from the "xri-authentication" member attribute in the "system-xri-supported" System Description attribute [PWG5100.22]. The following values are supported:

'certificate'; Authentication using Secure Sockets Layer (SSL) and Transport Layer Security (TLS) certificates. This is equivalent to the 'certificate' value for the "xri-authentication" member attribute.

'negotiate'; Kerberized authentication is required. This is equivalent to the 'negotiate' value for the "xri-authentication" member attribute.

'none'; No authentication is required. This is equivalent to the 'none' value for the "xri-authentication " member attribute.

'oauth'; OAuth 2.0 authentication is required using the Bearer method. This is equivalent to the 'oauth' value for the "xri-authentication " member attribute.

'username,password'; Username + password authentication is required. This is equivalent to the 'basic' or 'digest' values for the "xri-authentication " member attribute.

The default value for the "air" key is 'none'.

5.1.4.2 UUID

The REQUIRED "UUID" key provides the value of the "system-uuid" System Status attribute [PWG 5100.22] without the leading "urn:uuid:". For example, if a System reports a "system-uuid" value of:

```
urn:uuid:12345678-9ABC-DEF0-1234-56789ABCDEF0
```

The "UUID" key will have a value of:

```
12345678-9ABC-DEF0-1234-56789ABCDEF0
```

6. New Attributes

6.1 System Description Attributes

6.1.1 system-dns-sd-name (name(63))

This REQUIRED attribute provides the current DNS-SD service name for the System. For example, if this attribute contains "Example System" the System will register “Example System._ipps-system._tcp.local.”.

Systems that support changing the value using the Set-System-Attributes operation MUST list 'system-dns-sd-name' in the "system-settable-attributes-supported" System Description attribute [PWG5100.22]. When a new name is set, the System MUST re-register all DNS-SD services associated with it. However, if the new name causes a collision with other network devices, the System MUST replace the value set with a non-conflicting name as required by multicast DNS, typically by appending a unique number to the provided name.

Note: Changing the DNS-SD service name can prevent Clients from resolving the System's services if those Clients use a statically configured name for the System.

7. Conformance Requirements

7.1 System Conformance Requirements

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

1. The required discovery methods defined in section 5;
2. The required attribute defined in section 6;
3. The internationalization considerations defined in section 8; and
4. The security considerations defined in section 9.

7.2 Client Conformance Requirements

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

1. The required discovery methods defined in section 5;
2. The required attributes defined in section 6;
3. The internationalization considerations defined in section 8; and
4. The security considerations defined in section 9.

8. 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 Character Property Model [UTR23] – character properties

Unicode Conformance Model [UTR33] – Unicode conformance basis

9. Security Considerations

The IPP extensions defined in this document require the same security considerations as defined in the Internet Printing Protocol/1.1 [STD92].

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

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

10. IANA Considerations

10.1 Attribute Registrations

The attributes defined in this registration will be published by IANA according to the procedures in the Internet Printing Protocol/1.1 [STD92] in the following file:

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

The registry entries will contain the following information:

```
System Description attributes:                          Reference
--------------------------                              ---------
system-dns-sd-name(name(63))                            [IPPSYSDISC10]
```

10.2 Service Type Registration

The DNS-SD service type defined in this specification will be published by IANA according to the procedures in Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry [BCP165].

The registration template is as follows:

```
Service Name: ipps-system

Transport Protocol(s): tcp

Assignee/Contact: Michael Sweet, msweet@msweet.org

Description: Imaging System Services using the Internet Printing Protocol
over HTTPS.

Reference: https://ftp.pwg.org/pub/pwg/ipp/registrations/reg-ippsysdisc10-
20200604.pdf

Port Number: 631

Service Code:

Known Unauthorized Uses:

Assignment Notes: Change controller is The Printer Working Group, c/o The
IEEE Industry Standards and Technology Organization, 445 Hoes Lane,
Piscataway, NJ 08854, USA
```


11. References

11.1 Normative References

[BCP14] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119/BCP 14, March 1997, http://tools.ietf.org/html/rfc2119

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

[PWG5100.14] M. Sweet, "IPP Everywhere v1.1", PWG 5100.14-2020, ??? 2020, https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ippeve11-20200417.pdf

[PWG5100.22] M. Sweet, I. McDonald, "IPP System Service v1.0 (SYSTEM)", PWG 5100.22-2019, November 2019, https://ftp.pwg.org/pub/pwg/candidates/cs-ippsystem10-20191122-5100.22.pdf

[PWG5108.06] P. Zehler, "PWG System Object and System Control Service Semantics", PWG 5108.06-2012, February 2012, https://ftp.pwg.org/pub/pwg/candidates/cs-sm20-system10-20120217-5108.06.pdf

[RFC1876] C. Davis, P. Vixie, T. Goodwin, I. Dickinson, "A Means for Expressing Location Information in the Domain Name System", January 1996, RFC 1876, https://tools.ietf.org/html/rfc1876

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

[RFC6762] S. Cheshire, M. Krocmal, "Multicast DNS", RFC 6762, February 2013, https://tools.ietf.org/html/rfc6762

[RFC6763] S. Cheshire, M. Krocmal, "DNS-Based Service Discovery", RFC 6763, February 2013, https://tools.ietf.org/html/rfc6763

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

[STD63] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC 3629/STD 63, November 2003, http://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, http://tools.ietf.org/html/rfc3986

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

[UAX9] Unicode Consortium, “Unicode Bidirectional Algorithm”, UAX#9, February 2019, https://www.unicode.org/reports/tr9

[UAX14] Unicode Consortium, “Unicode Line Breaking Algorithm”, UAX#14, February 2019, https://www.unicode.org/reports/tr14

[UAX15] M. Davis, M. Duerst, "Unicode Normalization Forms", Unicode Standard Annex 15, February 2019, https://www.unicode.org/reports/tr15

[UAX29] Unicode Consortium, “Unicode Text Segmentation”, UAX#29, February 2019, https://www.unicode.org/reports/tr29

[UAX31] Unicode Consortium, “Unicode Identifier and Pattern Syntax”, UAX#31, February 2019, https://www.unicode.org/reports/tr31

[UNICODE] Unicode Consortium, "Unicode Standard", Version 12.0.0, March 2019, https://www.unicode.org/versions/Unicode12.0.0/

[UTS10] Unicode Consortium, “Unicode Collation Algorithm”, UTS#10, April 2019, https://www.unicode.org/reports/tr10

[UTS35] Unicode Consortium, “Unicode Locale Data Markup Language”, UTS#35, March 2019, https://www.unicode.org/reports/tr35

[UTS39] Unicode Consortium, “Unicode Security Mechanisms”, UTS#39, May 2019, https://www.unicode.org/reports/tr39

11.2 Informative References

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

[UTR23] Unicode Consortium “Unicode Character Property Model”, UTR#23, May 2015, https://www.unicode.org/reports/tr23

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

[UNISECFAQ] Unicode Consortium “Unicode Security FAQ”, November 2016, https://www.unicode.org/faq/security.html

12. Author's Addresses

Primary author:

Michael Sweet
Lakeside Robotics Corporation

