

Network Working Group
INTERNET-DRAFT
Updates: [2910](#), [2911](#) (if approved)
Intended Status: Standards Track
Expires: 18 June 2015

Ira McDonald
High North Inc
Michael Sweet
Apple Inc
18 December 2014

IPP over HTTPS Transport Binding and 'ipps' URI Scheme
draft-mcdonald-ipps-uri-scheme-18.txt

Abstract

This document defines the Internet Printing Protocol (IPP) over HTTPS transport binding and the corresponding 'ipps' URI scheme, that is used to designate the access to the network location of a secure IPP print service or a network resource managed by such a service.

This document defines an alternate IPP transport binding to that defined in the original IPP URL Scheme ([RFC 3510](#)), but this document does not update or obsolete [RFC 3510](#).

This document updates [RFC 2910](#) and [RFC 2911](#).

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#). Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/1id-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

This Internet-Draft will expire on 18 June 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

McDonald, Sweet

Expires 18 June 2015

[Page 1]

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1.	Introduction	4
1.1.	Structure of this Document	4
1.2.	Rationale for this Document	5
2.	Conventions Used in this Document	5
2.1.	Printing Terminology	5
3.	IPP over HTTPS Transport Binding	6
4.	Definition of 'ipps' URI Scheme	7
4.1.	Applicability of 'ipps' URI Scheme	7
4.2.	Syntax of 'ipps' URI Scheme	7
4.3.	Associated Port for 'ipps' URI Scheme	9
4.4.	Character Encoding of 'ipps' URI Scheme	9
4.5.	Examples of 'ipps' URI	9
4.6.	Comparisons of 'ipps' URI	10
5.	IANA Considerations	10
6.	Security Considerations	12
6.1.	Problem Statement	12
6.1.1.	Targets of Attacks	12
6.1.2.	Layers of Attacks	12
6.2.	Attacks and Defenses	13
6.2.1.	Faked 'ipps' URI	13
6.2.2.	Unauthorized Access by IPP Client	13
6.2.3.	Compromise at Application Layer Gateway	14
6.2.4.	No Client Authentication for 'ipps' URI	14
6.3.	TLS Version Requirements	14
7.	Acknowledgments	14
8.	References	15
8.1.	Normative References	15
8.2.	Informative References	16
9.	Appendix A - Abbreviations	17
10.	Authors' Addresses	18

1. Introduction

This document defines the Internet Printing Protocol (IPP) over HTTPS transport binding and the corresponding 'ipps' URI scheme, that is used to designate the access to the network location of a secure IPP print service or a network resource managed by such a service.

This document has been submitted to the IETF by the Internet Printing Protocol Working Group of the IEEE-ISTO Printer Working Group, as part of their PWG IPP Everywhere (PWG 5100.14) project for secure mobile printing with vendor-neutral Client software.

This document defines an alternate IPP transport binding to that defined in the original IPP URL Scheme [[RFC3510](#)], but this document does not update or obsolete [[RFC3510](#)].

This document updates:

- a) IPP/1.1 Encoding and Transport [[RFC2910](#)], by extending [section 4](#) 'Encoding of the Transport Layer', [section 5](#) 'IPP URL Scheme', and [section 8.2](#) 'Using IPP with TLS' to add the new standard URI scheme of 'ipps' for IPP Printers; and
- b) IPP/1.1 Model and Semantics [[RFC2911](#)], by extending [section 4.1.6](#) 'uriScheme' and [section 4.4.1](#) 'printer-uri-supported' to add the new standard URI scheme of 'ipps' for IPP Printers.

The following versions of IPP are currently defined:

- a) 1.0 in [[RFC2566](#)] (obsolete);
- b) 1.1 in [[RFC2911](#)];
- c) 2.0 in [[PWG5100.12](#)];
- d) 2.1 in [[PWG5100.12](#)]; and
- e) 2.2 in [[PWG5100.12](#)].

Overview information about IPP is available in [section 1 of RFC 2911](#) [[RFC2911](#)], [section 1 of RFC 3196](#) [[RFC3196](#)], and [section 1](#) of PWG IPP Version 2.0 Second Edition [[PWG5100.12](#)].

1.1. Structure of this Document

This document contains the following sections:

[Section 2](#) defines the conventions and terms used throughout the document.

[Section 3](#) defines the IPP over HTTPS transport binding.

[Section 4](#) defines the 'ipps' URI scheme.

McDonald, Sweet

Expires 18 June 2015

[Page 4]

Sections [5](#) and [6](#) contain IANA and security considerations, respectively.

[Section 7](#) contains acknowledgments.

[Section 8](#) contains references.

[1.2.](#) Rationale for this Document

The 'ipps' URI scheme was defined for the following reasons:

- 1) Some existing IPP Client and IPP Printer implementations of Upgrading to TLS Within HTTP/1.1 [[RFC2817](#)] are flawed and unreliable, although this is not due to specification defects in [[RFC2817](#)] itself.
- 2) Some existing IPP Client and IPP Printer implementations of HTTP Upgrade [[RFC2817](#)] do not perform upgrade at the beginning of every HTTP [[RFC7230](#)] connection, but instead only shift to secure IPP for selected IPP operations (inherently dangerous behavior on the same underlying TCP [[TCPROAD](#)] connection).
- 3) IPP Printer server-mandated HTTP Upgrade [[RFC2817](#)] can still lead to exposure of IPP Client data if the Expect request header is not used - basically the IPP Client can send its whole Print-Job request before the IPP Printer has a chance to respond and say, "Wait! You need to encrypt first!"

[2.](#) Conventions Used in this Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

[2.1.](#) Printing Terminology

The reader of this document needs to be familiar with the printing terms defined in IPP/1.1 Model and Semantics [[RFC2911](#)] as well as the following:

IPP Client: The software (on some hardware platform) that submits IPP Job creation and IPP Printer and IPP Job management operations via the IPP over HTTP transport binding defined in the IPP/1.1 Encoding and Transport [[RFC2910](#)] and/or the IPP over HTTPS transport

binding defined in [section 3](#) of this specification to an IPP Printer

McDonald, Sweet

Expires 18 June 2015

[Page 5]

(print spooler, print gateway, or physical printing device).

IPP Job: The set of attributes and documents for one print job instantiated in an IPP Printer.

IPP Job object: Synonym for IPP Job.

IPP Printer: The software (on some hardware platform) that receives IPP Job creation and IPP Printer and IPP Job management operations via the IPP over HTTP transport binding defined in the IPP/1.1 Encoding and Transport [[RFC2910](#)] and/or the IPP over HTTPS transport binding defined in [section 3](#) of this specification from an IPP Client.

IPP Printer object: Synonym for IPP Printer.

'ipps' URI: A URI using the 'ipps' URI scheme defined in [section 4](#) of this specification.

3. IPP over HTTPS Transport Binding

This document defines the following alternate IPP over HTTPS transport binding for the abstract protocol defined in IPP/1.1 Model and Semantics [[RFC2911](#)] and IEEE-ISTO PWG IPP Version 2.0 Second Edition [[PWG5100.12](#)].

When using an 'ipps' URI, an IPP Client MUST establish an IPP application layer connection according to the following sequence:

- 1) The IPP Client selects an 'ipps' URI value from "printer-uri-supported" Printer attribute [[RFC2911](#)], a directory entry, discovery info, a web page, etc.;
- 2) The IPP Client converts the 'ipps' URI to an 'https' URI [[RFC7230](#)] (replacing 'ipps' with 'https' and inserting the port number from the URI or port 631 if the URI doesn't include an explicit port number);
- 3) The IPP Client establishes an HTTPS [[RFC7230](#)] secure session layer connection to the target endpoint; and
- 4) The IPP Client sends requests to and receives responses from the target IPP application layer resource over the HTTPS [[RFC7230](#)] secure session layer connection using the POST method defined in [[RFC7231](#)].

McDonald, Sweet

Expires 18 June 2015

[Page 6]

4. Definition of 'ipps' URI Scheme

4.1. Applicability of 'ipps' URI Scheme

Per PWG IPP Everywhere [[PWG5100.14](#)], in IPP protocol exchanges, the 'ipps' URI scheme MUST only be used:

- a) To specify absolute URI for IPP secure print services and their associated network resources;
- b) To specify the use of the abstract protocol defined in IPP/1.1 Model and Semantics [[RFC2911](#)] and IEEE-ISTO PWG IPP Version 2.0 Second Edition [[PWG5100.12](#)]; and
- c) To specify the use of the transport binding defined in this document.

The 'ipps' URI scheme allows an IPP Client to choose an appropriate IPP secure print service (for example, from a directory). The IPP Client can establish an HTTPS connection to the specified IPP secure print service. The IPP Client can send IPP protocol requests (for example, 'Print-Job' requests) and receive IPP protocol responses over that HTTPS connection.

See: [Section 4.2](#) (syntax) of this document.

See: [Section 4.4.1](#) 'printer-uri-supported' in IPP/1.1 Model and Semantics [[RFC2911](#)].

See: [Section 5](#) 'IPP URL Scheme' in IPP/1.1 Encoding and Transport [[RFC2910](#)].

See: [Section 4](#) 'IPP Standards' of IEEE-ISTO PWG IPP Version 2.0 Second Edition [[PWG5100.12](#)].

4.2. Syntax of 'ipps' URI Scheme

The abstract protocol defined in IPP/1.1 Model and Semantics [[RFC2911](#)] places a limit of 1023 octets (NOT characters) on the length of a URI.

See: URI Generic Syntax [[STD66](#)].

Per PWG IPP Everywhere [[PWG5100.14](#)], for compatibility with existing IPP implementations, IPP Printers SHOULD NOT generate 'ipp' [[RFC3510](#)] or 'ipps' URI (or allow administrators to configure) lengths above 255 octets, because many older IPP Client implementations do not

properly support these lengths.

McDonald, Sweet

Expires 18 June 2015

[Page 7]

Per PWG IPP Everywhere [[PWG5100.14](#)], in IPP protocol exchanges, 'ipps' URI MUST be represented in absolute form. Absolute URI always begin with a scheme name followed by a colon. For definitive information on URI syntax and semantics, see "Uniform Resource Identifiers (URI) Generic Syntax and Semantics" [[STD66](#)]. This specification adopts the definitions of "host", "port", and "query" from [[STD66](#)]. This specification adopts the definition of "absolute-path" from [[RFC7230](#)].

The 'ipps' URI scheme syntax in ABNF [[STD68](#)] is defined as follows:

```
ipps-uri =  
  "ipps:" "/" host [ ":" port ] [ absolute-path [ "?" query ] ]
```

Per IPP/1.1 Encoding and Transport [[RFC2910](#)], if the port is empty or not given, then port 631 MUST be used.

See: [Section 4.3](#) (port) in this document.

The semantics are that the identified resource (see [[RFC7230](#)]) is located at the IPP secure print service listening for HTTPS connections on that port of that host; and the Request-URI for the identified resource is 'absolute-path'.

Note: The higher-level "authority" production is not imported from [[STD66](#)], because it includes an optional "userinfo" component which cannot be used in 'ipps' URI.

Note: The "query" production does not have defined semantics in IPP and was never used in examples in IPP/1.1 Encoding and Transport [[RFC2910](#)] or the original IPP URL Scheme [[RFC3510](#)]. The "query" is retained here for consistency, but IPP Clients SHOULD avoid its use (because the semantics would be implementation-defined).

Note: Per PWG IPP Everywhere [[PWG5100.14](#)], literal IPv4 or IPv6 addresses SHOULD NOT be used in 'ipps' URI, because:

- a) IP addresses are often changed after network device installation (for example, based on DHCP reassignment after a power cycle);
- b) IP addresses often don't map simply to security domains;
- c) IP addresses are difficult to validate with X.509 server certificates (because they do not map to common name or alternate name attributes); and
- d) IP link local addresses are not "portable" due to link identity

Per IPP/1.1 Encoding and Transport [[RFC2910](#)], if the 'absolute-path' is not present in an IPP URI, it MUST be given as "/" when used as a Request-URI for a resource (see [[RFC7230](#)]). An 'ipps' URI is transformed into an 'https' URI by replacing "ipps:" with "https:" and inserting port 631 (if an explicit 'port' is not present in the

original 'ipps' URI).

McDonald, Sweet

Expires 18 June 2015

[Page 8]

See: [Section 4.3](#) (port) in this document.

4.3. Associated Port for 'ipps' URI Scheme

Per IPP/1.1 Encoding and Transport [[RFC2910](#)], all 'ipps' URI which do NOT explicitly specify a port MUST be resolved to IANA-assigned well-known port 631, already registered in [[PORTREG](#)] by [[RFC2910](#)].

Note: Per direction of the IESG, as described in [[RFC2910](#)], port 631 is used for all IPP protocol connections (with or without TLS [[RFC5246](#)]). Port 631 is therefore used for both 'ipp' [[RFC3510](#)] and 'ipps' URI, which both refer to an IPP Printer or a network resource managed by an IPP Printer. IPP Printer implementors can refer to the CUPS [[CUPS](#)] source code for an example of incoming connection handling for the dual use of port 631.

See: IANA Port Numbers Registry [[PORTREG](#)].

See: IPP/1.1 Encoding and Transport [[RFC2910](#)].

4.4. Character Encoding of 'ipps' URI Scheme

Per PWG IPP Everywhere [[PWG5100.14](#)], 'ipps' URI MUST:

- a) Use the UTF-8 [[STD63](#)] charset for all components; and
- b) Use [[STD66](#)] rules for percent encoding data octets outside the US-ASCII coded character set [[ASCII](#)].

4.5. Examples of 'ipps' URI

The following are examples of well-formed 'ipps' URI for IPP Printers (for example, to be used as protocol elements in 'printer-uri' operation attributes of 'Print-Job' request messages):

```
ipps://example.com/  
ipps://example.com/ipp  
ipps://example.com/ipp/faxout  
ipps://example.com/ipp/print  
ipps://example.com/ipp/scan  
ipps://example.com/ipp/print/bob  
ipps://example.com/ipp/print/ira
```

Note: The use of an explicit 'ipp' path component followed by explicit 'print', 'faxout', 'scan', or other standard or vendor

service component is best practice per [[PWG5100.14](#)], [[PWG5100.15](#)],

McDonald, Sweet

Expires 18 June 2015

[Page 9]

and [[PWG5100.17](#)].

Each of the above URI is a well-formed URI for an IPP Printer and each would reference a logically different IPP Printer, even though some of those IPP Printers might share the same host system. Note that 'print' might represent some grouping of IPP Printers (for example, a load-balancing spooler), while the 'bob' or 'ira' last path components might represent two different physical printer devices, Or 'bob' and 'ira' might represent separate human recipients on the same physical printer device (for example, a physical printer supporting two job queues). In either case, both 'bob' and 'ira' would behave as different and independent IPP Printers.

The following are examples of well-formed 'ipps' URI for IPP Printers with (optional) ports and paths:

```
ipps://example.com/  
ipps://example.com/ipp/print  
ipps://example.com:631/ipp/print
```

The first and second 'ipps' URI above will be resolved to port 631 (IANA assigned well-known port for IPP). The second and third 'ipps' URI above are equivalent (see [section 4.6](#)).

See: [Section 4.2](#) (syntax) and [section 4.3](#) (port) in this document.

4.6. Comparisons of 'ipps' URI

Per PWG IPP Everywhere [[PWG5100.14](#)], when comparing two 'ipps' URI to decide if they match or not, an IPP Client MUST use the same rules as those defined for 'http' and 'https' URI comparisons in [[RFC7230](#)], with the single following exception:

- A port that is empty or not given MUST be treated as equivalent to the well-known port for that 'ipps' URI (port 631).

See: [Section 4.3](#) (port) in this document.

See: [Section 2.7.3](#) 'http and https URI Normalization and Comparison' in [[RFC7230](#)].

5. IANA Considerations

[RFC Editor: Replace 'xxxx' with assigned RFC number before publication]

IANA is asked to register the new keyword value 'ipps' for the IPP

McDonald, Sweet

Expires 18 June 2015

[Page 10]

Printer "printer-uri-supported" attribute in the IANA IPP Registry [IPPREG], per [section 6.2](#) Attribute Extensibility of IPP/1.1 [RFC2911] as follows:

IANA is asked to register the 'ipps' URI scheme using the following template, which conforms to [BCP35].

URI scheme name: ipps

Status: Permanent

URI scheme syntax: See [section 4.2](#) of RFC xxxx.

URI scheme semantics: The 'ipps' URI scheme is used to designate secure IPP Printer objects (print spoolers, print gateways, print devices, etc.) on Internet hosts accessible using the IPP protocol enhanced to support guaranteed data integrity and negotiable data privacy using TLS [RFC5246] as specified in HTTP/1.1 [RFC7230].

Encoding Considerations: See [section 4.4](#) of RFC xxxx.

Applications/protocols that use this URI scheme name:

The 'ipps' URI scheme is intended to be used by applications that need to access secure IPP Printers using the IPP protocol enhanced to support guaranteed data integrity and negotiable data privacy using TLS [RFC5246] as specified in HTTP/1.1 [RFC7230]. Such applications may include (but are not limited to) IPP-capable web browsers, IPP Clients that wish to print a file, and servers (for example, print spoolers) wishing to forward a Job for processing.

Interoperability Considerations: The widely deployed, open source IPP print service CUPS [CUPS] (on most UNIX, Linux, and Apple OS X systems) has supported 'ipps' URI for several years before the publication of this document. PWG IPP Everywhere [PWG5100.14] (IPP secure, mobile printing extensions) requires the use of 'ipps' URI for mandatory data integrity and negotiable data confidentiality.

Security Considerations: See [section 6](#) of RFC xxxx.

Contact:

Ira McDonald <blueroofmusic@gmail.com>

Michael Sweet <msweet@apple.com>

Author/Change controller:

IESG

McDonald, Sweet

Expires 18 June 2015

[Page 11]

References: [RFC 2910](#), [RFC 2911](#), RFC xxxx, and IEEE-ISTO PWG 5100.12.

6. Security Considerations

6.1. Problem Statement

Powerful mobile devices (laptops, tablets, smartphones, etc.) are now commonly used to access enterprise and Cloud print services across the public Internet. This is the primary use case for PWG IPP Everywhere [[PWG5100.14](#)], which has already been adopted by operating system and printer vendors and several other public standards bodies. End user and enterprise documents and user privacy-sensitive information are at greater risk than ever before. This IPP over HTTPS transport binding and 'ipps' URI scheme specification was defined to enable high availability combined with secure operation in this dynamic environment (for example, wireless hotspots in hotels, airports, and restaurants).

See: [Section 1](#) Introduction of [[PWG5100.14](#)].

See: [Section 3.1](#) Rationale of [[PWG5100.14](#)].

6.1.1. Targets of Attacks

A network print spooler (logical printer) or print device (physical printer) is potentially subject to attacks, which may target:

- a) The network (to compromise the routing infrastructure, for example, by creating congestion);
- b) The Internet Printing Protocol (IPP) [[RFC2911](#)] (for example, to compromise the normal behavior of IPP);
- c) The print job metadata (for example, to extract privacy-sensitive information from the job submission request or via query of the job on the IPP Printer); or
- d) The print document content itself (for example, to steal the data or to corrupt the documents being transferred).

6.1.2. Layers of Attacks

Attacks against print services can be launched:

- a) Against the network infrastructure (for example, TCP [[TCPROAD](#)] congestion control);

McDonald, Sweet

Expires 18 June 2015

[Page 12]

- b) Against the IPP data flow itself (for example, by sending forged packets or forcing TLS [[RFC5246](#)] version downgrade); or
- c) Against the IPP operation parameters (for example, by corrupting requested document processing attributes).

6.2. Attacks and Defenses

This 'ipps' URI Scheme specification adds the following additional security considerations to those described in [[RFC7230](#)], [[RFC2910](#)], [[RFC2911](#)], [[RFC5246](#)], [[RFC7230](#)], [[PWG5100.12](#)], and [[STD66](#)].

See: [Section 8](#) 'Security Considerations' in [[RFC2910](#)].

See: [Section 8](#) 'Security Considerations' in [[RFC2911](#)].

See: [Appendix D](#) 'Implementation Notes', [Appendix E](#) 'Backward Compatibility', and [Appendix F](#) 'Security Analysis' of [[RFC5246](#)].

See: [Section 10](#) 'Security Considerations' in [[PWG5100.12](#)].

See: [Section 7](#) 'Security Considerations' in [[STD66](#)].

6.2.1. Faked 'ipps' URI

An 'ipps' URI might be faked to point to a rogue IPP secure print service, thus collecting confidential job metadata or document contents from IPP Clients.

Due to administrator reconfiguration or physical relocation of an IPP Printer, a former literal IPv4 or IPv6 address might no longer be valid - see [section 4.2](#) for the recommendation against the use of literal IP addresses in 'ipps' URI.

Server authentication mechanisms and security mechanisms specified in IPP/1.1 Encoding and Transport [[RFC2910](#)], HTTP/1.1 [[RFC7230](#)], and TLS/1.2 [[RFC5246](#)] can be used to address this threat.

6.2.2. Unauthorized Access by IPP Client

An 'ipps' URI might be used to access an IPP secure print service by an unauthorized IPP Client, for example, extracting privacy-sensitive information such as "job-originating-user-name" job metadata defined in IPP/1.1 Model and Semantics [[RFC2911](#)].

Client authentication mechanisms and security mechanisms specified in

IPP/1.1 Encoding and Transport [[RFC2910](#)], HTTP/1.1 [[RFC7230](#)], and TLS/1.2 [[RFC5246](#)] can be used to address this threat.

6.2.3. Compromise at Application Layer Gateway

An 'ipps' URI might be used to access an IPP secure print service at a print protocol application layer gateway (for example, an IPP to LPD [[RFC1179](#)] gateway [[RFC2569](#)]), potentially causing silent compromise of IPP security mechanisms.

There is no general defense against this threat by an IPP Client. System administrators SHOULD avoid such configurations.

6.2.4. No Client Authentication for 'ipps' URI

An 'ipps' URI does not define parameters to specify the required IPP Client authentication mechanism (for example, 'certificate' as defined in [section 4.4.2](#) 'uri-authentication-supported' of IPP Model [[RFC2911](#)]).

An IPP Client SHOULD first use service discovery or directory protocols (e.g., the LDAP Printer Schema [[RFC3712](#)]) or directly send an IPP Get-Printer-Attributes operation to the target IPP Printer to read "printer-uri-supported", "uri-authentication-supported", and "uri-security-supported" attributes to discover the required IPP Client authentication and security mechanisms for each supported URI.

6.3. TLS Version Requirements

Per PWG IPP Everywhere [[PWG5100.14](#)] (and in accordance with security best practices and all existing deployments of the 'ipps' URI scheme), IPP Clients and IPP Printers that support this specification MUST use TLS/1.2 [[RFC5246](#)] or higher version, for all 'ipps' secure transport layer connections.

Implementors will find useful advice in Recommendations for Secure Use of TLS and DTLS [[TLSBCP](#)].

7. Acknowledgments

This document has been submitted to the IETF by the Internet Printing Protocol Working Group of the IEEE-ISTO Printer Working Group, as

part of their PWG IPP Everywhere [[PWG5100.14](#)] project for secure

McDonald, Sweet

Expires 18 June 2015

[Page 14]

mobile printing with vendor-neutral Client software.

This document defines an alternate IPP transport binding to that defined in the original IPP URL Scheme [[RFC3510](#)], but this document does not update or obsolete [[RFC3510](#)].

Thanks to Claudio Allochio, Jari Arrko, Spencer Dawkins, Adrian Farrel, Tom Hastings, Bjoern Hoerhmann, Smith Kennedy, Graham Klyne, Barry Leiba, S. Mooneswamy, Kathleen Moriarty, Sandra Murphy, Tom Petch, Pete Resnick, Benson Schliesser, Robert Sparks, Jerry Thrasher, Mykyta Yevstifeyev, Pete Zehler, and the members of the IEEE-ISTO PWG IPP WG.

8. References

8.1. Normative References

- [ASCII] "American National Standards Institute, Coded Character Set -- 7-bit American Standard Code for Information Interchange", ANSI X3.4, 1986.
- [PWG5100.12] Bergman, R., Lewis, H., McDonald, I., and M. Sweet, "Internet Printing Protocol Version 2.0 Second Edition (IPP/2.0 SE)", PWG 5100.12, February 2011.
<<http://www.pwg.org/standards.html>>
- [PWG5100.14] McDonald, I. and M. Sweet, "PWG IPP Everywhere", PWG 5100.14, January 2013.
<<http://www.pwg.org/standards.html>>
- [RFC2119] Bradner, S., Key words for use in RFCs to Indicate Requirement Levels, [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2910] Herriot, R., Ed., Butler, S., Moore, P., Turner, R., and J. Wenn, "Internet Printing Protocol/1.1: Encoding and Transport", [RFC 2910](#), September 2000.
- [RFC2911] Hastings, T., Ed., Herriot, R., deBry, R., Isaacson, S., and P. Powell, "Internet Printing Protocol/1.1: Model and Semantics", [RFC 2911](#), September 2000.
- [RFC5246] Dierks, T., and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [RFC 5246](#), August 2008.
- [RFC7230] Fielding, R., and J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", [RFC 7230](#), June

2014.

McDonald, Sweet

Expires 18 June 2015

[Page 15]

- [RFC7231] Fielding, R., and J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", [RFC 7231](#), June 2014.
- [STD63] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, [RFC 3629](#), November 2003.
- [STD66] Berners-Lee, T., Fielding, R., and L. Masinter, Uniform Resource Identifiers (URI) Generic Syntax, STD 66, [RFC 3986](#), January 2005.
- [STD68] Crocker, D., Ed., and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, [RFC 5234](#), January 2008.

8.2. Informative References

- [BCP35] Hansen, T., Hardie, T., and L. Masinter, "Guidelines and Registration Procedures for New URI Schemes", [BCP 35](#), [RFC 4395](#), February 2006.
- [CUPS] Apple, "CUPS standards-based, open source printing system for OS X and other UNIX-like operating systems"
<<https://www.cups.org/>>
- [IPPREG] Internet Assigned Numbers Authority (IANA) Registries
"Internet Printing Protocol"
<<http://www.iana.org/assignments/ipp-registrations/>>
- [PORTREG] Internet Assigned Numbers Authority (IANA) Registries
"Port Numbers"
<<http://www.iana.org/assignments/port-numbers>>
- [PWG5100.15] M. Sweet, "PWG IPP FaxOut Service", PWG 5100.15, June 2014.
<<http://www.pwg.org/standards.html>>
- [PWG5100.17] P. Zehler, "PWG IPP Scan Service", PWG 5100.17, September 2014.
<<http://www.pwg.org/standards.html>>
- [RFC1179] McLaughlin, L., "Line Printer Daemon Protocol", [RFC 1179](#), August 1990.
- [RFC2566] deBry, R., Hastings, T., Herriot, R., Isaacson, S., and P. Powell, "Internet Printing Protocol/1.0: Model and Semantics", [RFC 2566](#), April 1999.

McDonald, Sweet

Expires 18 June 2015

[Page 16]

- [RFC2569] Herriot, R., Ed., Hastings, T., Jacobs, N., and J. Martin, "Mapping between LPD and IPP Protocols", [RFC 2569](#), April 1999.
- [RFC2817] Khare, R. and S. Lawrence, "Upgrading to TLS Within HTTP/1.1", [RFC 2817](#), May 2000.
- [RFC3196] Hastings, T., Manros, C., Zehler, P., Kugler, C., and H. Holst, "Internet Printing Protocol/1.1: Implementor's Guide", [RFC 3196](#), November 2001.
- [RFC3510] Herriot, R. and I. McDonald, "Internet Printing Protocol/1.1: IPP URL Scheme", [RFC 3510](#), April 2003.
- [RFC3712] Fleming, P. and I. McDonald, "Lightweight Directory Access Protocol (LDAP): Schema for Printer Services", [RFC 3712](#), February 2004.
- [TCPROAD] Duke, M., Braden, R., Eddy, W., Blanton, E., and A. Zimmerman, "A Roadmap for Transmission Control Protocol (TCP) Specification Documents", work in progress, <<https://datatracker.ietf.org/doc/draft-ietf-tcpm-tcp-rfc4614bis/>>
- [TLSBCP] Scheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of TLS and DTLS", work in progress, <<https://datatracker.ietf.org/doc/draft-ietf-uta-tls-bcp/>>

9. [Appendix A](#) - Abbreviations

This document makes use of the following abbreviations (given with their expanded forms and references for further reading):

- ABNF - Augmented Backus-Naur Form [[STD68](#)]
- ASCII - American Standard Code for Information Interchange [[ASCII](#)]
- HTTP - HyperText Transfer Protocol [[RFC7230](#)]
- HTTPS - HTTP over TLS [[RFC7230](#)]
- IANA - Internet Assigned Numbers Authority
<<http://www.iana.org>>
- IEEE - Institute of Electrical and Electronics Engineers
<<http://www.ieee.org>>

McDonald, Sweet

Expires 18 June 2015

[Page 17]

- IESG - Internet Engineering Steering Group
<<http://www.ietf.org/iesg/>>
- IPP - Internet Printing Protocol [[RFC2911](#)] and [[PWG5100.12](#)]
<<http://www.pwg.org/ipp/>>
- ISTO - IEEE Industry Standards and Technology Organization
<<http://www.ieee-isto.org/>>
- LPD - Line Printer Daemon Protocol [[RFC1179](#)]
- PWG - IEEE-ISTO Printer Working Group
<<http://www.pwg.org>>
- RFC - Request for Comments
<<http://www.rfc-editor.org/rfc.html>>
- TCP - Transmission Control Protocol [[TCPROAD](#)]
- TLS - Transport Layer Security [[RFC5246](#)]
- URI - Uniform Resource Identifier [[STD66](#)]
- URL - Uniform Resource Locator [[STD66](#)]
- UTF-8 - Unicode Transformation Format - 8-bit [[STD63](#)]

10. Authors' Addresses

Ira McDonald
High North Inc
221 Ridge Ave
Grand Marais, MI 49839

Phone: +1 906-494-2434
Email: blueroofmusic@gmail.com

Michael Sweet
Apple Inc
1 Infinite Loop, M/S 111-HOMC
Cupertino, CA 95014

Email: msweet@apple.com

Usage questions and comments on this 'ipps' URI Scheme can be sent directly to the editors at their above addresses and also to the PWG

IPP WG mailing list. Instructions for subscribing to the PWG IPP WG mailing list can be found at:

PWG IPP WG Web Page: <http://www.pwg.org/ipp/>

[PWG](#) IPP WG Mailing List: ipp@pwg.org

PWG IPP WG Subscription: <http://www.pwg.org/mailhelp.html>

Implementers of this specification are encouraged to join the PWG IPP WG Mailing List in order to participate in any discussions of clarification issues and comments. Note that this IEEE-ISTO PWG mailing list rejects mail from non-subscribers (in order to reduce spam).

