IPP Encrypted Jobs and Documents v1.0
(TRUSTNOONE)

Status: Interim

Abstract: This IPP Registration defines new encrypted IPP message formats that provide IPP with end-to-end encryption of IPP Job Template attributes, Document Template attributes, and Document data.


This document is available electronically at:


Copyright © 2018 The Printer Working Group. All rights reserved.
Copyright © 2018 The Printer Working Group. All rights reserved.

Title: IPP Encrypted Jobs and Documents v1.0 (TRUSTNOONE)

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.

Deleted: This document may be copied and furnished to others, and derivative works that comment on, or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice, this paragraph and the title of the Document as referenced below are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the IEEE-ISTO and the Printer Working Group, a program of the IEEE-ISTO.

Deleted: The IEEE-ISTO and the Printer Working Group DISCLAIM ANY AND ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. The Printer Working Group, a program of the IEEE-ISTO, reserves the right to make changes to the document without further notice. The document may be updated, replaced or made obsolete by other documents at any time. The IEEE-ISTO takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. The IEEE-ISTO invites any interested party to bring to its attention any copyrights, patents, or patent applications, or other proprietary rights which may cover technology described in this document.

The IEEE-ISTO takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. The IEEE-ISTO invites any interested party to bring to its attention any copyrights, patents, or patent applications, or other proprietary rights which may cover technology described in this document.

The IEEE-ISTO takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. The IEEE-ISTO invites any interested party to bring to its attention any copyrights, patents, or patent applications, or other proprietary rights which may cover technology described in this document.

The IEEE-ISTO takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. The IEEE-ISTO invites any interested party to bring to its attention any copyrights, patents, or patent applications, or other proprietary rights which may cover technology described in this document.

The IEEE-ISTO takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. The IEEE-ISTO invites any interested party to bring to its attention any copyrights, patents, or patent applications, or other proprietary rights which may cover technology described in this document.
Table of Contents

167 1. Introduction ......................................................................................................................... 5
169 2. Terminology ....................................................................................................................... 5
170 2.1 Conformance Terminology .............................................................................................. 5
171 2.2 Printing Terminology ....................................................................................................... 5
172 2.3 Protocol Role Terminology ............................................................................................. 6
173 2.4 Other Terminology ........................................................................................................... 6
174 2.5 Acronyms and Organizations ......................................................................................... 7
175 3. Requirements ..................................................................................................................... 8
176 3.1 Rationale for IPP Encrypted Jobs and Documents ......................................................... 8
177 3.2 Use Cases ......................................................................................................................... 8
178 3.2.1 Printing Encrypted Document Locally on Printer....................................................... 8
179 3.2.2 Pull Print Encrypted Document from Print Service to Local Printer ......................... 8
180 3.3 Exceptions ....................................................................................................................... 9
181 3.3.1 Unauthorized Access to Document Data ................................................................. 9
182 3.3.2 Signed Document Modified ....................................................................................... 9
183 3.4 Out of Scope .................................................................................................................... 9
184 3.5 Design Requirements ...................................................................................................... 9
185 4. Model .................................................................................................................................. 11
186 4.1 Printer Behavior ............................................................................................................... 11
187 4.2 Proxy Behavior ................................................................................................................ 11
188 4.3 Client Behavior ............................................................................................................... 12
189 5. Document Formats .......................................................................................................... 12
190 5.1 application/ipp+pgp-encrypted ....................................................................................... 12
191 5.2 application/ipp+pkcs7-encrypted ................................................................................... 12
192 6. Printer Description Attributes ......................................................................................... 12
193 6.1 pgp-document-format-supported (1setOf mimeMediaType) ............................................ 12
194 6.2 pkcs7-document-format-supported (1setOf mimeMediaType) ....................................... 13
195 6.3 printer-pgp-public-key (1setOf text(MAX)) ................................................................. 13
196 6.4 printer-pgp-repertoire-configured (type2 keyword) ...................................................... 13
197 6.5 printer-pgp-repertoire-supported (1setOf type2 keyword) ............................................. 13
198 6.6 printer-pkcs7-public-key (1setOf text(MAX)) ............................................................... 13
199 6.7 printer-pkcs7-repertoire-configured (type2 keyword) ................................................... 13
200 6.8 printer-pkcs7-repertoire-supported (1setOf type2 keyword) ........................................ 13
201 7. Additional Semantics for Existing Operations ................................................................. 14
202 7.1 Print-Job and Send-Document: Encrypted IPP Message Data ....................................... 14
203 8. Conformance Requirements ............................................................................................. 14
204 8.1 Printer Conformance Requirements .............................................................................. 14
205 8.2 Infrastructure Printer Conformance Requirements ........................................................ 14
206 8.3 Client Conformance Requirements ............................................................................. 15
207 8.4 Proxy Conformance Requirements .............................................................................. 15
208 9. Internationalization Considerations ............................................................................... 15
209 10. Security Considerations ................................................................................................ 16
210 11. IANA Considerations ..................................................................................................... 17
211 11.1 Attribute Registrations ............................................................................................... 17
212 11.2 Attribute Value Registrations .................................................................................... 17
1. Introduction

This IPP Registration defines new encrypted IPP message formats that provide IPP with end-to-end encryption of IPP Job Template attributes, Document Template attributes, and Document data. The encrypted formats use public key cryptography with an optional password to effectively protect the IPP message/Document data payload from intermediaries and when the data is at rest in the destination Output Device.

The new message formats reuse the existing OpenPGP [RFC4880] and S/MIME [RFC5751] message formats to protect the combination of IPP message and document data normally sent in the clear as part of a Job Creation Request.

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 [RFC2119]. The term CONDITIONALLY REQUIRED is additionally defined for a conformance requirement that applies to a particular capability or feature.

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 [RFC2911].

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

This document also defines the following protocol roles in order 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 Other Terminology

- **Certificate**: A type that binds an entity's name to a Public Key with a Digital Signature [RFC5751].

- **Digital Signature**: A cryptographic hash of data (a Certificate, a Document, a message, etc.) that has been associated with an entity that can be verified mathematically, for example by using Public-Key Encryption.

- **One-Time Pad**: A symmetric encryption key that is randomly generated and is used to encrypt or decrypt a single message.

- **OpenPGP**: Security software using PGP 5.x [RFC4880]

- **Private Key**: The recipient's key value in Public-Key Encryption.

- **Public Key**: The sender's key value in Public-Key Encryption.

- **Public-Key Encryption**: An encryption technique that uses a paired (asymmetric) key algorithm for secure data communication. Messages are encrypted with one key value and decrypted using the other key value, so the security of the technique depends on verifying that the first key originated from the intended recipient. This is typically done by comparing a cryptographic hash (Digital Signature) of the recipient's Certificate against a hash that was encrypted using the second key.

- **Symmetric-Key Encryption**: An encryption technique that uses a single (symmetric) key algorithm for secure data communication. Messages are encrypted and decrypted with the same secret key value, so the security of the technique depends on the confidentiality of the key. This is typically done by using One-Time Pads.
2.5 Acronyms and Organizations

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

3.1 Rationale for IPP Encrypted Jobs and Documents

Existing specifications define the following:

1. The Internet Printing Protocol/1.1: Model and Semantics defines the "document-format" attribute.

2. "Internet Printing Protocol (IPP) over HTTPS Transport Binding and the 'ipps' URI Scheme" defines the IPP over HTTPS transport binding, which provides session transport encryption.

This IPP Registration defines a new IPP convention for encrypting Jobs and Documents by:

1. Defining a set of standard encrypted IPP message formats that securely convey Job and Document information;

2. Defining new IPP Printer Description attributes that convey information about the encryption capabilities of the Printer; and


3.2 Use Cases

3.2.1 Printing Encrypted Document Locally on Printer

Garrett is visiting a client and needs to print a sensitive document but wants to be sure that a print job with the document is not readable if it is recovered from the printer or print server, and that he can detect whether it has been changed.

Garrett chooses a printer supporting end-to-end encryption, makes his job choices, enters a passcode for the print job, and taps "Print" to submit his choices. The client software validates the public key of the receiving printer, encrypts the print job request using the public key and passcode, and sends it to the printer. Garrett then goes to the printer and enters his passcode, allowing the printer to decrypt the print job using his passcode and the corresponding private key.

3.2.2 Pull Print Encrypted Document from Print Service to Local Printer

Helen is on the train, viewing a document on her tablet and wants to print a copy when she gets to work. Helen taps the control to print the document, and a print dialog UI is presented on the tablet's screen. Her tablet is configured with a printer that is a personal account on a cloud print service. She selects that to be the target printer, chooses "Encrypt Job" in the
The design requirements for this registration are:

1. Define IPP attributes and values to describe the supported encryption methods and public keys.
2. Define amended semantics for all affected IPP operations.
3. Register all new IPP attributes, attribute keywords, attribute enum values, operations, and other IPP specific values in the IANA IPP registry.
4. Define security requirements necessary to support encrypted Jobs and Documents.

5. Define MIME media types for providing encrypted IPP Job Template and Document Template attributes along with Document data, and

6. Register all new MIME media types in the IANA MIME Media Type registry.

The design recommendations for this registration are:

1. Define best-practices for user experience.
4. Model

This document defines a new encrypted printing model where the Printer provides attributes to the Client containing a Certificate to use for encryption. Clients then use the Certificate (and optionally a User-supplied passphrase) to produce an encrypted IPP message containing the operation, Job Template, and Document Template attributes along with the associated Document data. The encrypted message is sent in a Print-Job or Send-Document request as the request's Document data. Because the encrypted IPP message uses Public-Key Encryption, it can only be decrypted by the entity that possesses the Private Key corresponding to the provided Certificate and (if used) the User passphrase. Because this model encapsulates the encrypted data as a Document, it does not offer support for encrypted Print Jobs that use the Print-URI or Send-URI operations. However, such Jobs can still use traditional access control mechanisms (authentication, passwords, etc.) to protect access to sensitive Document data.

TODO: Talk about how to get encrypted Job Receipt, if we decide to do that.

4.1 Printer Behavior

When enabled, the Printer MUST provide a Certificate for each of the supported encrypted message formats along with the supported and configured End User password repertoire in the Printer Description attributes defined in section 6. If decryption and processing is performed by the Printer, it MUST also provide a list of document formats that are supported inside encrypted IPP messages.

When a Print-Job or Send-Document request is received, the Printer validates any attributes that are provided in the unencrypted portion of the IPP message and defers additional validation and processing until the Job moves to the 'processing' state and the Document data can be decrypted. Document data MUST remain encrypted when the Job is not in the 'processing' or 'processing-stopped' states.

When the Printer is acting as an Infrastructure Printer [PWG5100.18] and the Certificate and repertoire information is supplied by the Proxy, the Printer does no additional validation or processing of the Document data and MUST pass the Document data to the Proxy without decryption or alteration.

Printers can require encrypted Print Jobs by listing only the encrypted IPP message formats in the "document-format-supported" Printer Description attribute.

4.2 Proxy Behavior

A Proxy [PWG5100.18] for a Printer that conforms to this registration provides the Infrastructure Printer with the Certificates, repertoire, and document format values using the Update-Output-Device-Attributes operation. If the Proxy has access to the corresponding Private Keys, it MUST NOT provide them to the Infrastructure Printer.
Proxies can require encrypted Print Jobs by reporting only the encrypted IPP message formats in the "document-format-supported" Printer Description attribute supplied in the Update-Output-Device-Attributes request.

4.3 Client Behavior

When an End User initiates a print action, the Client software will query the Printer's capabilities and status using the Get-Printer-Attributes request. If the response contains the attributes listed in section 6, the Client software can either automatically encrypt the Job Creation Request or offer the End User the option to do so.

As part of the encryption process, Clients SHOULD allow End Users to provide a passphrase conforming to the Printer's configured password repertoire.

5. Document Formats

5.1 application/ipp+pgp-encrypted

This MIME media type consists of an IPP message ("application/ipp") followed by Document data that is stored inside an OpenPGP message [RFC4880]. The symmetric key for the message is encrypted using the Public Key from the "printer-pgp-public-key (1setOf text(MAX))" Printer Description attribute (section 6.3) and any passphrase supplied by the End User as described in section 3.7.2.2 of [RFC4880].

5.2 application/ipp+pkcs7-encrypted

This MIME media type consists of an IPP message ("application/ipp") followed by Document data that is stored inside an S/MIME message [RFC5751]. The symmetric key for the message is encrypted using the Public Key from the "printer-pkcs7-public-key (1setOf text(MAX))" Printer Description attribute (section 6.3) and any passphrase supplied by the End User as described in section 3.2 of [RFC5751].

TODO: Add application/ipp+pgp-signed and application/ipp+pkcs7-signed if we need them.

6. Printer Description Attributes

6.1 ppg-document-format-supported (1setOf mimeMediaType)

The "ppg-document-format-supported" Printer Description attribute specifies the set of Document formats that can be embedded in Document data of type "application/ipp+pgp-encrypted".

Deleted: Several new document formats are defined for IPP Encrypted Jobs and Documents. These new document formats indicate the nature of the contents of the files to a very small degree. They are grouped by the encrypted document formats on which they are based.

IPP Encrypted Payload

Deleted: An IPP Encrypted Payload consists of an "application/pgp-encrypted" segment followed by an optional second segment. The format of the second segment is specified by the value of the "document-format" attribute from the IPP segment. The "document-format" attribute MUST be present in the IPP segment if there is an optional second segment. The payload conveyed by all the encrypted formats defined in this IPP Registration document MUST contain an "IPP Encrypted Payload" [application/ipp-pgp-encrypted]

The "application/ipp-pgp-encrypted" Media Type is an OpenPGP "application/pgp-encrypted" format [RFC3156] containing an IPP Encrypted Payload. The "application/ipp-pgp-sig" Media Type is an OpenPGP "application/pgp-signature" format file [RFC3156] containing an IPP Encrypted Payload. The "application/ipp-pkcs7-mime" Media Type is

Deleted: 5.1

Deleted: document

Deleted: included

Deleted: in a byte stream

Page 12 of 22 Copyright © 2018 The Printer Working Group. All rights reserved.
6.2 pkcs7-document-format-supported (1setOf mimeMediaTypetype)

This attribute specifies the set of Document formats that can be embedded in Document data of type "application/ipp-pkcs7-encrypted".

6.3 printer-pgp-public-key (1setOf text(MAX))

This attribute specifies the PGP public key to use when encrypting IPP requests using PGP.

6.4 printer-pgp-repertoire-configured (type2 keyword)

This attribute specifies the password repertoire currently configured in the Printer. The value of this attribute MUST be one of the set of values specified by the Printer's "printer-pgp-repertoire-supported" attribute. A supporting Client can use this attribute's value to limit User input when encrypting the symmetric key for PGP.

6.5 printer-pgp-repertoire-supported (1setOf type2 keyword)

This attribute specifies the repertoires the Printer can be configured to use if the Printer supports an additional passphrase at the Printer console. Any keyword registered for use with "job-password-repertoire-supported" can be listed.

6.6 printer-pkcs7-public-key (1setOf text(MAX))

This attribute specifies the X.509 public key to use when encrypting IPP requests using S/MIME.

6.7 printer-pkcs7-repertoire-configured (type2 keyword)

This attribute specifies the password repertoire currently configured in the Printer. The value of this attribute MUST be one of the set of values specified by the Printer's "printer-pkcs7-repertoire-supported" attribute. A supporting Client can use this attribute's value to limit User input when encrypting the symmetric key for S/MIME.

6.8 printer-pkcs7-repertoire-supported (1setOf type2 keyword)

This attribute specifies the repertoires the Printer can be configured to use if the Printer supports an additional passphrase at the Printer console. Any keyword registered for use with "job-password-repertoire-supported" can be listed.
7. Additional Semantics for Existing Operations

7.1 Print-Job and Send-Document: Encrypted IPP Message Data

This registration adds additional semantics when a Client submits Document data in the format 'application/ipp+pgp-encrypted' or 'application/ipp+pkcs7-encrypted'. When supplied, the Printer that decrypts the data for processing MUST:

3. Merge any attributes in the encrypted message with the attributes provided in the unencrypted portion of the original request,
4. Validate the combined request attributes as required for a standard request, and
5. Abort or continue processing the Job using the merged attributes.

When merging attributes, the values of encrypted attributes take precedence since a Client MAY send obfuscated values in the unencrypted portion of the request, e.g., "requesting-user-name" and "job-name".

8. Conformance Requirements

8.1 Printer Conformance Requirements

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

1. The ‘application/ipp+pgp-encrypted’ and/or ‘application/ipp+pkcs7-encrypted’ MIME media types defined in section 5;
2. The PGP and/or S/MIME attributes and values defined in section 6;
3. The additional semantics defined in section 7;
4. The internationalization considerations defined in section 9; and
5. The security considerations defined in section 10.

8.2 Infrastructure Printer Conformance Requirements

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

1. The restrictions on processing of encrypted data as defined in section 4.1;
2. The ‘application/ipp+pgp-encrypted’ and/or ‘application/ipp+pkcs7-encrypted’ MIME media types defined in section 5;
3. The PGP and/or S/MIME attributes and values defined in section 6;
4. The additional semantics defined in section 7;
5. The internationalization considerations defined in section 9; and
6. The security considerations defined in section 10.

8.3 Client Conformance Requirements

In order for a Client to claim conformance to this document, a Client MUST support:
7. The 'application/ipp+pgp-encrypted' and/or 'application/ipp+pkcs7-encrypted' MIME media types defined in section 5;
8. The PGP and/or S/MIME attributes and values defined in section 6;
9. The internationalization considerations defined in section 9; and
10. The security considerations defined in section 10.

8.4 Proxy Conformance Requirements

In order for a Proxy to claim conformance to this document, a Proxy MUST support:
11. The 'application/ipp+pgp-encrypted' and/or 'application/ipp+pkcs7-encrypted' MIME media types defined in section 5;
12. The PGP and/or S/MIME attributes and values defined in section 6;
13. The additional semantics defined in section 7;
14. The internationalization considerations defined in section 9; and
15. The security considerations defined in section 10.

9. 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

10. 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].

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

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

11. IANA Considerations

11.1 Attribute Registrations

The attributes defined in this document will be published by IANA according to the procedures in IPP/1.1 Model and Semantics [RFC2911] section 6.2 in the following file:

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

The registry entries will contain the following information:

<table>
<thead>
<tr>
<th>Printer Description attributes:</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp-document-format-supported (lsetOf mimeMediaType)</td>
<td>[TRUSTNOONE]</td>
</tr>
<tr>
<td>printer-ppp-public-key (lsetOf text(MAX))</td>
<td>[TRUSTNOONE]</td>
</tr>
<tr>
<td>printer-ppp-repertoire-configured (type2 keyword)</td>
<td>[TRUSTNOONE]</td>
</tr>
<tr>
<td>printer-ppp-repertoire-supported (lsetOf type2 keyword)</td>
<td>[TRUSTNOONE]</td>
</tr>
</tbody>
</table>

11.2 Attribute Value Registrations

The attributes defined in this document will be published by IANA according to the procedures in IPP/1.1 Model and Semantics [RFC2911] section 6.1 in the following file:

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

The registry entries will contain the following information:

<table>
<thead>
<tr>
<th>Attributes (attribute syntax)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keyword Attribute Value</td>
<td>-----------</td>
</tr>
<tr>
<td>printer-ppp-repertoire-configured (type2 keyword)</td>
<td>[TRUSTNOONE]</td>
</tr>
<tr>
<td>&lt; all printer-ppp-repertoire-supported values &gt;</td>
<td>[TRUSTNOONE]</td>
</tr>
<tr>
<td>printer-ppp-repertoire-supported (lsetOf type2 keyword)</td>
<td>[TRUSTNOONE]</td>
</tr>
<tr>
<td>&lt; all job-password-repertoire-supported values &gt;</td>
<td>[IPPWG20160229-1]</td>
</tr>
</tbody>
</table>

11.3 Status Code Registrations

The attributes defined in this document will be published by IANA according to the procedures in IPP/1.1 Model and Semantics [RFC2911] section 6.6 in the following file:

https://www.iana.org/assignments/ipp-registrations
The registry entries will contain the following information:

<table>
<thead>
<tr>
<th>Value</th>
<th>Status</th>
<th>Code Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0400:0x04FF - Client Error:</td>
<td></td>
<td></td>
<td>[REFERENCE]</td>
</tr>
<tr>
<td>0x04XX client-error-name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x0500:0x05FF - Server Error:</td>
<td></td>
<td></td>
<td>[REFERENCE]</td>
</tr>
<tr>
<td>0x05XX server-error-name</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12. References

12.1 Normative References

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Author(s)</th>
<th>Reference</th>
</tr>
</thead>
</table>


1281 12.2 Informative References

13. Authors' Addresses

Primary authors:

Smith Kennedy  
HP Inc.  
11311 Chinden Blvd. MS 506  
Boise, ID 83714  
smith.kennedy@hp.com

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

The authors would also like to thank the following individuals for their contributions to this standard:

Ira McDonald - High North, Inc.

14. Appendix A: File Formats Considered

The following file formats were considered in the development of this IPP Registration. Some were selected while others were left out.
14.1 OpenPGP

The OpenPGP file format, defined in [RFC4880], has been used for signing and encrypting email message bodies as well as arbitrary file content. PGP depends on a "web of trust" trust model to establish trust but may also derive trust from more centralized trust models.

14.2 S/MIME

The S/MIME file format, defined in [RFC5751], is primarily used for signing and encrypting email message body content. Its cryptography is based on existing public key infrastructure (PKI) and depends on certificates issued by known certificate authorities (CAs) for establishing trust.

14.3 ZIP Archive

The ZIP archive file format has encryption features, but the password-based encryption is weak, and implementations that support public key cryptography suffer from interoperability problems.

15. Change History

15.1 March 28, 2018

1. Updated to current IPP Registration template.
2. Abstract: Simplified
3. Section 1: Rewrote
4. Section 2: Added/updated terminology
5. Section 3: Updated use cases, exceptions, out-of-scope, and requirements
6. Section 4: Model, talk about how it all works together
7. Section 5: Rewrite as application/ipp+pgp-encrypted and application/ipp+pkcs7-encrypted
8. Section 6: Added S/MIME attributes, normalized to current template style
9. Section 7: Added amended semantics for Print-Job and Send-Document
10. Section 8: Expanded to spell out separate requirements for Printers, Infrastructure Printers, Clients, and Proxies
11. Section 9: Added security considerations
12. Section 10: Updated with all of the current attributes and amended
13. Updated all references.

15.2 February 19, 2018

Moved back to using Microsoft Word format. Incorporates product of feedback from February 2018 PWG virtual F2F meeting and content from a slide set presented at that meeting by

1502 **15.3 February 5, 2018**

1503 Resurrected and updated with more current scheme, where the encryption attributes are now conveyed using new IPP attributes rather than embedded within the document format itself. Also rewrote the use cases and requirements to rekindle discussion about scope and possible solutions.

1507 **15.4 February 4, 2015**

1508 Initial revision, presented at PWG February 2015 F2F.
The IEEE-ISTO and the Printer Working Group DISCLAIM ANY AND ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

The Printer Working Group, a program of the IEEE-ISTO, reserves the right to make changes to the document without further notice. The document may be updated, replaced or made obsolete by other documents at any time.

The IEEE-ISTO takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights.

The IEEE-ISTO invites any interested party to bring to its attention any copyrights, patents, or patent applications, or other proprietary rights which may cover technology that may be required to implement the contents of this document. The IEEE-ISTO and its programs shall not be responsible for identifying patents for which a license may be required by a document and/or IEEE-ISTO Industry Group Standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention. Inquiries may be submitted to the IEEE-ISTO by e-mail at: ieee-isto@ieee.org.

The Printer Working Group acknowledges that the IEEE-ISTO (acting itself or through its designees) is, and shall at all times, be the sole entity that may authorize the use of certification marks, trademarks, or other special designations to indicate compliance with these materials.

Use of this document is wholly voluntary. The existence of this document does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to its scope.
About the IEEE-ISTO

The IEEE-ISTO is a not-for-profit corporation offering industry groups an innovative and flexible operational forum and support services. The IEEE-ISTO provides a forum not only to develop standards, but also to facilitate activities that support the implementation and acceptance of standards in the marketplace. The organization is affiliated with the IEEE (http://www.ieee.org/) and the IEEE Standards Association (http://standards.ieee.org/).

For additional information regarding the IEEE-ISTO and its industry programs visit:

http://www.ieee-isto.org

About the IEEE-ISTO PWG

The Printer Working Group (or PWG) is a Program of the IEEE Industry Standards and Technology Organization (ISTO) with member organizations including printer manufacturers, print server developers, operating system providers, network operating systems providers, network connectivity vendors, and print management application developers. The group is chartered to make printers and the applications and operating systems supporting them work together better. All references to the PWG in this document implicitly mean “The Printer Working Group, a Program of the IEEE ISTO.” In order to meet this objective, the PWG will document the results of their work as open standards that define print related protocols, interfaces, procedures and conventions. Printer manufacturers and vendors of printer related software will benefit from the interoperability provided by voluntary conformance to these standards.

In general, a PWG standard is a specification that is stable, well understood, and is technically competent, has multiple, independent and interoperable implementations with substantial operational experience, and enjoys significant public support.

For additional information regarding the Printer Working Group visit:

http://www.pwg.org

Contact information:

The Printer Working Group
c/o The IEEE Industry Standards and Technology Organization
445 Hoes Lane
Piscataway, NJ 08854
USA
About the Internet Printing Protocol Workgroup

The Internet Printing Protocol (IPP) Workgroup has developed a modern, full-featured network printing protocol, which is now the industry standard. IPP allows a print client to query a printer for its supported capabilities, features, and parameters to allow the selection of an appropriate printer for each print job. IPP also provides job information prior to, during, and at the end of job processing.

For additional information regarding IPP visit:

http://www.pwg.org/ipp/

Implementers of this specification are encouraged to join the IPP Workgroup mailing list in order to participate in any discussions of the specification. Suggested additions, changes, or clarification to this specification, should be sent to the IPP Workgroup mailing list for consideration.

---

Document using a scheme supported by the Printer using the authentication credential provided by Garrett, creates a new Job on the target Printer, and adds the now-encrypted Document to the Job.

---

The Document can only be decrypted by the Printer when Garrett provides the credential to the Printer to allow the Job to be processed.

---

Herbert is a disenchanted IT administrator who wishes to examine everybody's print jobs and sends each print job's document content to a repository for later examination. Herbert is unable to read the document recovered from Garrett's Job because the Document was encrypted.

---

Push Print Encrypted Document from Print Service to Local Printer

Violet is at the park during her lunch break, viewing a document on her phone, and wants to print a copy when she gets back to work. Violet taps the control to print the document, and a print dialog UI is presented on the phone's screen. Her phone is configured with a Printer that is a personal account on a cloud print service. Violet selects that to be the target printer, chooses “Encrypt Job” in the printing options presented, and specifies a credential to be used for encryption. Violet then taps “Print”, causing the document to be encrypted and sent to her cloud print service account.

Later, Violet arrives at the office, she goes to a Printer that she identifies as one that can receive jobs from her cloud print service. Violet opens her phone, authenticates with the cloud print service, chooses the Document or the Job containing the Document and taps
“Print”. The phone asks for a target printer, and Violet specifies the printer next to her. The Document arrives at the Printer, still encrypted. The Printer asks for the credential to decrypt the Document, and Violet provides that to the Printer. The Printer decrypts and prints the Document, and Violet collects it from the output bin.

**Symmetric (Shared Key) Encryption**

Duncan wants to encrypt his printed documents using a simple password. He selects a Printer that supports symmetric encryption, and it prompts him for a password. He provides one, and the document is encrypted using that password. A new Job containing a rendering of his print-ready Document is created and submitted to the Printer. When he gets to the printer itself, he scans his badge on a reader on the Printer, which contains that certificate's public key, which allows the Printer to decrypt the Document content and proceed with printing it.

**Asymmetric (PKI) Encryption**

Caleb's employer has configured his and other employees' accounts so that their print job document content can be encrypted for end-to-end encryption using their employer-issued X.509 certificate. Caleb chooses a printer supporting this encryption system, and his Client encrypts his Job's Document content using his certificate's private key. When he gets to the printer itself, Caleb scans his badge on a reader on the Printer, which contains that certificate's public key, which allows the Printer to decrypt the Document content and proceed with printing it.

The following design requirements shall be met by solutions specified in this document:

Selecting one or more document formats that support the following criteria:

- An encrypted payload
- Digital signature(s)
- Metadata describing the document format itself, as well as other information such as parameters used for the document encryption
- An evolving set of encryption parameters algorithms, hash algorithms, etc. that don't need to be designed or maintained by the PWG
- Can evolve to align with current best practices and state of the art techniques without having to re-specify new formats
Selecting one of the document formats identified in (1) to be a mandatory format that all printers supporting IPP Encrypted Jobs and Documents must support, to ensure baseline interoperability.

Replicating pertinent document metadata via IPP attributes to allow IPP operations to retrieve the metadata without retrieving the document itself.

Support for both symmetric and asymmetric encryption systems.

Ensuring that IPP can convey a normalized set of document encryption options using IPP attributes.

Design the system so that both the printable document content as well as...

Semantic Model Registrations

The extensions defined in this specification and provided in the following file:


will be added to the PWG Semantic Model XML schema.

OR

Except as noted below, the IPP attributes, values, and operations defined in this specification and listed in the preceding sections will be added to the PWG Semantic Model XML schema using the method defined in section 21 of [PWG5108.07].

Table 1 lists the attributes that are mapped to alternate element names.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Element Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>AlternateName</td>
</tr>
<tr>
<td>name-supported</td>
<td>Capabilities/AlternateName</td>
</tr>
</tbody>
</table>

Table 2 lists the values that are mapped to alternate Well-Known Values.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Value</th>
<th>Well-Known Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>value-1</td>
<td>AlternateValue1</td>
</tr>
<tr>
<td>name</td>
<td>value-2</td>
<td>AlternateValue2</td>
</tr>
</tbody>
</table>

Table 3 lists the operations that are mapped to alternate operation names.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Value</th>
<th>Well-Known Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>value-1</td>
<td>AlternateValue1</td>
</tr>
<tr>
<td>name</td>
<td>value-2</td>
<td>AlternateValue2</td>
</tr>
</tbody>
</table>
### IPP Operation Name | Semantic Model Operation Name
---|---
Operation-Get-Name | AlternateGet Name
Operation-Set-Name | Alternate Set Name


