The Printer Working Group

March 28, 2018
IPP Registration

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 a PWG Working Draft. For a definition of a "PWG Working Draft", see:

https://ftp.pwg.org/pub/pwg/general/pwg-process30.pdf

This document is available electronically at:

https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ipptrustnoone10-20180328.docx
https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ipptrustnoone10-20180328.pdf

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

Table of Contents

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/

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

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

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

3. Requirements

3.1 Rationale 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. Defining amended IPP Job and Document operation semantics for encrypted IPP messages.

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

printing options presented, and specifies a credential to be used for encryption. She then taps “Print”, and the document is encrypted and sent to her cloud print service account.

Later, when Helen arrives at the office, she goes to a printer that she identifies as one that can pull jobs from her cloud print service. Helen chooses the document or the job containing the document and taps “Print”. The printer asks for the credential to decrypt the document and Helen provides that to the printer. The printer decrypts and prints the document, and Helen collects it from the output bin.

3.3 Exceptions

3.3.1 Unauthorized Access to Document Data

Herbert is a disenchanted IT administrator who wishes to examine everyone's print jobs and sends each print job's document content to a repository for later examination. Herbert is unable to read the encrypted documents because he does not have the private key or passcode associated with the print job.

3.3.2 Signed Document Modified

Garrett prints another document and the document is changed by some entity at some stage in the print system between the client and the printer. The printer notifies Garrett that the document has been changed. Garrett chooses to abandon the output since it can no longer be trusted.

3.4 Out of Scope

The following are considered out of scope for this document:

1. Authentication infrastructure that may be used by the Printer, such as LDAP or RADIUS, and
2. Definition of the method for loading public and private keys on a Printer.

3.5 Design Requirements

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 pgp-document-format-supported (1setOf mimeMediaType)

The "pgp-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".

6.2 pkcs7-document-format-supported (1setOf mimeMediaType)

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 End 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 End 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:

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

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:

```
Printer Description attributes:                          Reference
-------------------------------                          ---------
pgp-document-format-supported (1setOf mimeMediaType)     [TRUSTNOONE]
printer-pgp-public-key (1setOf text(MAX))                [TRUSTNOONE]
printer-pgp-repertoire-configured (type2 keyword)        [TRUSTNOONE]
printer-pgp-repertoire-supported (1setOf type2 keyword)  [TRUSTNOONE]
```

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:

```
Attributes (attribute syntax)
  Keyword Attribute Value                                Reference
  -----------------------                                ---------
printer-pgp-repertoire-configured (type2 keyword)        [TRUSTNOONE]
  < all printer-pgp-repertoire-supported values >        [TRUSTNOONE]
printer-pgp-repertoire-supported (1setOf type2 keyword)  [TRUSTNOONE]
  < all job-password-repertoire-supported values >       [IPPWG20160229-1]
```

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:

```
Value    Status Code Name                                    Reference
------   ------------------------------------------------    ---------
0x0400:0x04FF - Client Error:
  0x04XX client-error-name                                   [REFERENCE]
0x0500:0x05FF - Server Error:
  0x05XX server-error-name                                   [REFERENCE]
```

12. References

12.1 Normative References

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

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

[PWG5100.12] R. Bergman, H. Lewis, I. McDonald, M. Sweet, "IPP/2.0 Second Edition", PWG 5100.12-2011, February 2011, https://ftp.pwg.org/pub/pwg/candidates/cs-ipp20-20110214-5100.12.pdf

[PWG5100.18] M. Sweet, I. McDonald, "IPP Shared Infrastructure Extensions (INFRA)", PWG 5100.18-2015, June 2015, https://ftp.pwg.org/pub/pwg/candidates/cs-ippinfra10-20150619-5100.18.pdf

[RFC4880] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, R. Thayer, "OpenPGP Message Format", RFC 4880, November 2007, https://tools.ietf.org/html/rfc4880

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

[RFC5751] B. Ramsdell, S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010, https://tools.ietf.org/html/rfc5751

[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

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

[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

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

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

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

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

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

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

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

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

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

12.2 Informative References

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

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

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

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

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

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

Mike Sweet (https://ftp.pwg.org/pub/pwg/ipp/slides/ipp-document-encryption-february-18.pdf).

15.3 February 5, 2018

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.

15.4 February 4, 2015

Initial revision, presented at PWG February 2015 F2F.

