The Printer Working Group

April 18, 2019
IPP Registration

IPP Encrypted Jobs and Documents v1.0 (TRUSTNOONE)

Status: Interim

Abstract: This specification defines new encrypted IPP message formats and operations that provide IPP with end-to-end encryption of IPP Job attributes, Document 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-ipptrustnoone10-20190418.docx
https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ipptrustnoone10-20190418.pdf

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

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 system providers, network connectivity vendors, and print management application developers. The PWG 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.”

To meet this objective, the PWG documents the results of their work as open standards that define print related protocols, interfaces, procedures, and conventions. A PWG standard is a stable, well understood, and technically competent specification that is widely used with multiple independent and interoperable implementations. Printer manufacturers and vendors of printer related software benefit from the interoperability provided by voluntary conformance to these standards.

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

Table of Contents

1. Introduction 6
2. Terminology 6
2.1 Conformance Terminology 6
2.2 Printing Terminology 6
2.3 Protocol Role Terminology 7
2.4 Other Terminology 7
2.5 Acronyms and Organizations 9
3. Requirements 10
3.1 Rationale 10
3.2 Use Cases 10
3.2.1 Printing Encrypted Document Locally on Printer 10
3.2.2 Pull Print Encrypted Document from Print Service to Local Printer 10
3.2.3 Query Job Receipt After Printing 11
3.3 Exceptions 11
3.3.1 Unauthorized Access to Document Data 11
3.3.2 Signed Document Modified 11
3.4 Out of Scope 11
3.5 Design Requirements 11
4. Model 13
4.1 Printer Behavior 13
4.2 Proxy Behavior 14
4.3 Client Behavior 14
5. Document Formats 14
5.1 application/ipp+pgp-encrypted 14
6. Operations 15
6.1 Acknowledge-Encrypted-Job-Attributes 15
6.1.1 Acknowledge-Encrypted-Job-Attributes Request 15
6.1.2 Acknowledge-Encrypted-Job-Attributes Response 16
6.2 Fetch-Encrypted-Job-Attributes 16
6.2.1 Fetch-Encrypted-Job-Attributes Request 16
6.2.2 Fetch-Encrypted-Job-Attributes Response 17
6.3 Get-Encrypted-Job-Attributes 18
6.3.1 Get-Encrypted-Job-Attributes Request 18
6.3.2 Get-Encrypted-Job-Attributes Response 18
7. Attributes 19
7.1 Operation Attributes 19
7.1.1 encrypted-job-request-format (mimeMediaType) 19
7.1.2 encrypted-job-request-id (integer(1:MAX)) 19
7.1.3 requesting-user-pgp-public-key (1setOf text(MAX)) 19
7.2 Printer Description Attributes 20
7.2.1 pgp-document-format-supported (1setOf mimeMediaType) 20
7.2.2 printer-pgp-public-key (1setOf text(MAX)) 20
7.2.3 printer-pgp-repertoire-configured (type2 keyword) 20
7.2.4 printer-pgp-repertoire-supported (1setOf type2 keyword) 20
8. Additional Semantics for Existing Operations 20

8.1 Print-Job and Send-Document: Encrypted IPP Message Data 20
9. Additional Values for Existing Attributes 21
9.1 printer-state-reasons (1setOf type2 keyword) 21
10. Conformance Requirements 21
10.1 Printer Conformance Requirements 21
10.2 Infrastructure Printer Conformance Requirements 21
10.3 Client Conformance Requirements 21
10.4 Proxy Conformance Requirements 22
11. Internationalization Considerations 22
12. Security Considerations 23
12.1 PGP Cipher Suite Considerations 23
12.2 Unicode Considerations 23
13. IANA Considerations 23
13.1 Attribute Registrations 23
13.2 Type2 keyword Registrations 24
13.3 Type2 enum Registrations 24
13.4 Operation Registrations 24
13.5 MIME Media Type Registration 25
14. References 26
14.1 Normative References 26
14.2 Informative References 27
15. Authors' Addresses 28
16. Appendix A: File Formats Considered 28
16.1 OpenPGP 28
16.2 S/MIME 29
16.3 ZIP Archive 29
17. Change History 30
17.1 April 18, 2019 30
17.2 January 31, 2019 30
17.3 March 28, 2018 31
17.4 February 19, 2018 31
17.5 February 5, 2018 31
17.6 February 4, 2015 32

1. Introduction

This specification defines new encrypted IPP message formats that provide IPP with end-to-end encryption of IPP Job attributes, Document 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] message format 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 [STD92].

Document: An object created and managed by a Printer that contains the description, processing, and status information. A Document object may have attached data and is bound to a single Job.

Job: An object created and managed by a Printer that contains description, processing, and status information. The Job also contains zero or more Document objects.

Logical Device: a print server, software service, or gateway that processes jobs and either forwards or stores the processed job or uses one or more Physical Devices to render output.

Output Device: a single Logical or Physical Device

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

2.3 Protocol Role Terminology

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.

Encrypted Job: A Job whose Document data, Job Receipt, and Job Ticket are encrypted using a public key so that only the recipient of the information can access it.

Job Receipt: The Job Status attributes that provide a summary of the work performed by the Printer such as the owner, state, dates and times, actual values used for Job Template attributes, and work counters.

Job Ticket: The operation and Job Template attributes supplied in a Job Creation request.

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

Existing specifications define the following:

1. The Internet Printing Protocol/1.1[STD92] defines the "document-format" attribute.
2. "Internet Printing Protocol (IPP) over HTTPS Transport Binding and the 'ipps' URI Scheme" **Error! Reference source not found.** defines the IPP over HTTPS transport binding which provides session transport encryption.

This specification 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;
3. Defining amended IPP Job and Document operation semantics for encrypted IPP messages; and
4. Defining new operations for transferring Encrypted Job Receipts.

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.

3.2.3 Query Job Receipt After Printing

Jane wishes to query the job receipts of a printer in order to do accounting of encrypted print jobs for the day. She uses her client software to send a query for the job receipt of each encrypted job, providing her public key and authentication credentials to the printer. The printer then validates her credentials and returns an encrypted job receipt using her public key. Her client software then decrypts the job receipt using her private key and retrieves the needed accounting information from the decrypted receipt.

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 specification 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 specification 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 of messages from the Client to the Printer. Clients then use the Printer Certificate (and optionally a User-supplied Certicate and/or passphrase) to produce an encrypted IPP message containing the operation, Job Template, and/or 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 Printer's 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.

Clients can request an Encrypted Job Receipt using a supplied User Certificate, subject to the Printer's access control policies. The contents of the Encrypted Job Receipt are only guaranteed to be stable once the Job reaches a terminating state, just as for regular Job Receipts.

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 7.2. 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.

As part of the Print-Job and Send-Document request, Clients include the End User's Public Key in the encrypted portion of the request. Printers use this Public Key to authenticate the Client in subsequent Get-Encrypted-Job-Attributes requests.

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 specification 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.

If supported by the Infrastructure Printer, Proxies receive notifications when a Client has requested an Encrypted Job Receipt. When such an event occurs, the Proxy fetches the Encrypted Job request, generates the Encrypted Job Receipt, and acknowledges the request with the attached Encrypted Job Receipt.

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 7.2, the Client software can either automatically encrypt the Job Creation Request or offer the End User the option to do so. When encrypting the request message, the Client generates a single session key which is encrypted only using the Printer's Public Key. The End User's Public Key is provided as an operation attribute in the encrypted request message, allowing the Printer to authenticate the Client in a subsequent Get-Encrypted-Job-Attributes request.

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 7.2.2) and any passphrase supplied by the End User as described in section 3.7.2.2 of [RFC4880].

6. Operations

6.1 Acknowledge-Encrypted-Job-Attributes

This operation is sent by a Proxy to acknowledge the receipt of an Encrypted Job attributes request from a Client that was retrieved using a Fetch-Encrypted-Job-Attributes request. Infrastructure Printers that support Encrypted Jobs MUST support this operation.

6.1.1 Acknowledge-Encrypted-Job-Attributes Request

The following groups of attributes are part of an Acknowledge-Encrypted-Job-Attributes request:

Group 1: Operation Attributes

"attributes-charset" (charset) and
"attributes-natural-language" (naturalLanguage):

The Client MUST supply and the Printer MUST support both of these attributes.

Target:

The "printer-uri" (uri) operation attribute which is the target Printer for the operation.

"output-device-uuid" (uri):

The Proxy MUST supply and the Infrastructure Printer MUST support this attribute which provides the identity of the Output Device for the request.

"encrypted-job-request-id" (integer(1:MAX)):

The Proxy MUST supply and the Infrastructure Printer MUST support this attribute that specifies which Encrypted Job request is being acknowledged.

"encrypted-job-request-format" (mimeMediaType):

The Proxy MUST supply and the Infrastructure Printer MUST support this attribute that specifies the Encrypted Job Receipt format.

Group 2: Encrypted Job Receipt Message

The Encrypted Job Receipt message.

6.1.2 Acknowledge-Encrypted-Job-Attributes Response

The following groups of attributes are part of an Acknowledge-Encrypted-Job-Attributes response:

Group 1: Operation Attributes

"attributes-charset" (charset) and
"attributes-natural-language" (naturalLanguage):

The Printer MUST return both of these attributes.

"status-message" (text(255)) and/or
"detailed-status-message" (text(MAX)):

The Printer MAY return one or both of these attributes.

Group 2: Unsupported Attributes

See [RFC8011] for details on returning Unsupported Attributes.

Group 3: Printer Attributes

"printer-state-reasons" (1setOf type2 keyword):

The state of the Infrastructure Printer after processing the request. Clients can look for the presence of the 'encrypted-job-request' keyword to know whether to send another Fetch-Encrypted-Job-Attributes request.

6.2 Fetch-Encrypted-Job-Attributes

This operation allows a Proxy to fetch a request for Encrypted Job attributes from the Client. The Infrastructure Printer

6.2.1 Fetch-Encrypted-Job-Attributes Request

The following groups of attributes are part of a Fetch-Encrypted-Job-Attributes request:

Group 1: Operation Attributes

"attributes-charset" (charset) and
"attributes-natural-language" (naturalLanguage):

The Client MUST supply and the Printer MUST support both of these attributes.

Target:

The "printer-uri" (uri) operation attribute which is the target Printer for the operation.

"output-device-uuid" (uri):

The Proxy MUST supply and the Infrastructure Printer MUST support this attribute which provides the identity of the Output Device for the request.

6.2.2 Fetch-Encrypted-Job-Attributes Response

The following groups of attributes are part of a Fetch-Encrypted-Job-Attributes response:

Group 1: Operation Attributes

"attributes-charset" (charset) and
"attributes-natural-language" (naturalLanguage):

The Printer MUST return both of these attributes.

"status-message" (text(255)) and/or
"detailed-status-message" (text(MAX)):

The Printer MAY return one or both of these attributes.

"job-id" (integer(1:MAX)):

The Job identifier for the Printer.

"encrypted-job-request-id" (integer(1:MAX)):

A unique identifier for the Encrypted Job request is being fetched.

"requested-attributes" (1setOf keyword):

The requested attributes sent by the Client to the Infrastructure Printer that specify which attributes the Client would like returned.

"requesting-user-name" (name(MAX)) and "requesting-user-uri" (uri):

The name and URI of the User requesting the attributes.

"requesting-user-pgp-public-key" (1setOf text(MAX)):

The PGP public key supplied by the Client to be used for encrypting the Job attributes.

Group 2: Unsupported Attributes

See [RFC8011] for details on returning Unsupported Attributes.

6.3 Get-Encrypted-Job-Attributes

This attribute allows a Client to query Encrypted Job attributes from a Printer. Once authorized, the attributes are encrypted using the Public Key supplied by the Client and returned as data following the IPP response.

If the supplied Public Key does not match the one supplied in the corresponding Print-Job or Send-Document request (section 8.1) or a Public Key that has been registered with the Printer through some means outside of IPP (e.g., for Administrators or Operators), the Printer MUST reject the request with the 'client-error-forbidden' status code.

6.3.1 Get-Encrypted-Job-Attributes Request

The following groups of attributes are part of a Get-Encrypted-Job-Attributes request:

Group 1: Operation Attributes

"attributes-charset" (charset) and
"attributes-natural-language" (naturalLanguage):

The Client MUST supply and the Printer MUST support both of these attributes.

Target:

The "printer-uri" (uri) and "job-id" (integer(1:MAX)) operation attributes which are the target Job for the operation.

"requested-attributes" (1setOf keyword):

The Client MAY supply and the Printer MUST support this attribute which specifies the attributes the Client would like returned.

"requesting-user-name" (name(MAX)) and "requesting-user-uri" (uri):

The name and URI of the User requesting the attributes.

"requesting-user-pgp-public-key" (1setOf text(MAX)):

The PGP public key supplied by the Client to be used for encrypting the Job attributes.

6.3.2 Get-Encrypted-Job-Attributes Response

The following groups of attributes are part of an Get-Encrypted-Job-Attributes response:

Group 1: Operation Attributes

"attributes-charset" (charset) and
"attributes-natural-language" (naturalLanguage):

The Printer MUST return both of these attributes.

"status-message" (text(255)) and/or
"detailed-status-message" (text(MAX)):

The Printer MAY return one or both of these attributes.

"encrypted-job-request-format" (mimeMediaType):

The Printer MUST return this attribute that specifies the Encrypted Job Receipt format.

Group 2: Unsupported Attributes

See [RFC8011] for details on returning Unsupported Attributes.

Group 3: Encrypted Job Receipt Message

The Encrypted Job Receipt message.

7. Attributes

7.1 Operation Attributes

7.1.1 encrypted-job-request-format (mimeMediaType)

This attribute specifies the MIME media type for the Encrypted Job attributes message.

7.1.2 encrypted-job-request-id (integer(1:MAX))

This attribute specifies a unique request identifier for the Acknowledge-Encrypted-Job-Attributes and Fetch-Encrypted-Job-Attributes operations.

7.1.3 requesting-user-pgp-public-key (1setOf text(MAX))

This attribute specifies the PGP public key to use when encrypting the IPP Job Receipt using PGP. The values are concatenated to form the Base64-encoded PGP public key block.

7.2 Printer Description Attributes

7.2.1 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".

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

This attribute specifies the PGP public key to use when encrypting IPP requests using PGP. The values are concatenated to form the Base64-encoded PGP public key block.

7.2.3 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.

7.2.4 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.

8. Additional Semantics for Existing Operations

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

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

1. Merge any attributes in the encrypted message with the attributes provided in the unencrypted portion of the original request,
2. Validate the combined request attributes as required for a standard request, and
3. 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".

Clients MUST include the "requesting-user-pgp-public-key" (section 7.1.3) operation attribute in the encrypted Document data.

9. Additional Values for Existing Attributes

9.1 printer-state-reasons (1setOf type2 keyword)

This specification adds the 'encrypted-job-attributes-requested' keyword, which is present when one or more Get-Encrypted-Job-Attributes requests are pending on an Infrastructure Printer.

10. Conformance Requirements

10.1 Printer Conformance Requirements

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

1. The 'application/ipp+pgp-encrypted' MIME media type defined in section 5;
2. The Get-Encrypted-Job-Attributes operation as defined in section 6;
3. The attributes and values defined in section 7.2;
4. The additional semantics defined in section 8;
5. The internationalization considerations defined in section 11; and
6. The security considerations defined in section 12.

10.2 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' MIME media type defined in section 5;
3. The Acknowledge-Encrypted-Job-Attributes, Fetch-Encrypted-Job-Attributes, and Get-Encrypted-Job-Attributes operations as defined in section 6;
4. The attributes and values defined in section 7.2;
5. The additional semantics defined in section 8;
6. The additional values defined in section 9;
7. The internationalization considerations defined in section 11; and
8. The security considerations defined in section 12.

10.3 Client Conformance Requirements

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

1. The 'application/ipp+pgp-encrypted' MIME media type defined in section 5;
2. The Get-Encrypted-Job-Attributes operation as defined in section 6;
3. The attributes and values defined in section 7.2;
4. The internationalization considerations defined in section 11; and

5. The security considerations defined in section 12.

10.4 Proxy Conformance Requirements

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

1. The 'application/ipp+pgp-encrypted' MIME media type defined in section 5;
2. The Acknowledge-Encrypted-Job-Attributes and Fetch-Encrypted-Job-Attributes operations as defined in section 6;
3. The attributes and values defined in section 7.2;
4. The additional semantics defined in section 8;
5. The additional values defined in section 9;
6. The internationalization considerations defined in section 11; and
7. The security considerations defined in section 12.

11. Internationalization Considerations

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

- The Universal Character Set (UCS) Transformation Format -- 8 bit (UTF-8) [STD63] encoding of Unicode [UNICODE] [ISO10646]; and

- The Unicode Format for Network Interchange [RFC5198] which requires transmission of well-formed UTF-8 strings and recommends transmission of normalized UTF-8 strings in Normalization Form C (NFC) [UAX15].

Unicode NFC is defined as the result of performing Canonical Decomposition (into base characters and combining marks) followed by Canonical Composition (into canonical composed characters wherever Unicode has assigned them).

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

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

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

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

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

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

- Unicode Identifier and Pattern Syntax [UAX31] – identifier use and normalization
- Unicode Collation Algorithm [UTS10] – sorting
- Unicode Locale Data Markup Language [UTS35] – locale databases

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

- Unicode Character Encoding Model [UTR17] – multi-layer character model
- Unicode Character Property Model [UTR23] – character properties
- Unicode Conformance Model [UTR33] – Unicode conformance basis

12. Security Considerations

The following sub-sections define security considerations in addition to those defined in the Internet Printing Protocol/1.1 [STD92].

12.1 PGP Cipher Suite Considerations

Clients and Printers MUST use modern cipher suites with Authenticated Encryption with Associated Data (AEAD).

12.2 Unicode Considerations

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

13. IANA Considerations

13.1 Attribute Registrations

The attributes defined in this document will be published by IANA according to the procedures in the Internet Printing Protocol/1.1 [STD92] 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]
```

13.2 Type2 keyword Registrations

The attributes defined in this document will be published by IANA according to the procedures in the Internet Printing Protocol/1.1 [STD92] 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 >           [TRUSTNOONE]
printer-state-reasons (1setOf type2 keyword)                 [RFC8011]
  encrypted-job-attributes-requested                         [TRUSTNOONE]
```

13.3 Type2 enum Registrations

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

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

The registry entries will contain the following information:

```
Attributes (attribute syntax)
  Enum Value      Enum Symbolic Name                         Reference
  ----------      ------------------                         ---------
operations-supported (1setOf type2 enum)                     [RFC8011]
  0x0068          Acknowledge-Encrypted-Job-Attributes       [TRUSTNOONE]
  0x0069          Fetch-Encrypted-Job-Attributes             [TRUSTNOONE]
  0x006A          Get-Encrypted-Job-Attributes               [TRUSTNOONE]
```

13.4 Operation Registrations

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

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

The registry entries will contain the following information:

Operation Name	Reference
Acknowledge-Encrypted-Job-Attributes	[TRUSTNOONE]
Fetch-Encrypted-Job-Attributes	[TRUSTNOONE]
Get-Encrypted-Job-Attributes	[TRUSTNOONE]
Print-Job(extension)	[TRUSTNOONE]
Send-Document(extension)	[TRUSTNOONE]

13.5 MIME Media Type Registration

The MIME media type defined in this white paper will be published by IANA according to the procedures in the Media Type Specifications and Registration Procedures [BCP13] in the following file:

https://www.iana.org/assignments/media-types

The registry will contain the following information:

```
Type name: application

Subtype name: ipp+pgp-encrypted

Required parameters: N/A

Optional parameters: N/A

Encoding considerations: Binary

Security considerations: Same as application/pgp-encrypted

Interoperability considerations: Same as for application/pgp-encrypted and
application/ipp

Published specification: [this specification]

Applications that use this media type: IPP

Fragment identifier considerations: N/A

Additional information:

  Deprecated alias names for this type: N/A
  Magic number(s): N/A
  File extension(s): N/A
  Macintosh file type code(s): N/A

Person & email address to contact for further information: Michael Sweet,
msweet@apple.com
```



```
Intended usage: COMMON

Restrictions on usage: N/A

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

Provisional registration? (standards tree only): No
```

14. References

14.1 Normative References

[BCP13] N. Freed, J. Klensin, T. Hansen, "Media Type Specifications and Registration Procedures", RFC 6838/BCP 13, January 2013, https://tools.ietf.org/html/bcp14

[BCP14] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119/BCP 14, March 1997, https://tools.ietf.org/html/bcp14

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

[PWG5100.12] M. Sweet, I. McDonald, "IPP Version 2.0, 2.1, and 2.2", PWG 5100.12-2015, October 2015, https://ftp.pwg.org/pub/pwg/standards/std-ipp20-20151030-5100.12.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, https://tools.ietf.org/html/rfc5198

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

[STD63] F. Yergeau, "UTF-8, a transformation format of ISO 10646", RFC 3629/STD 63, November 2003, https://tools.ietf.org/html/std63

[STD66] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", RFC 3986/STD 66, January 2005, https://tools.ietf.org/html/std66

[STD92] M. Sweet, I. McDonald, "Internet Printing Protocol/1.1", STD 92, January 2017, https://tools.ietf.org/html/std92

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

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

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

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

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

[UNICODE] Unicode Consortium, "Unicode Standard", Version 11.0.0, June 2018, https://www.unicode.org/versions/Unicode11.0.0/

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

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

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

14.2 Informative References

[EFAIL] D. Poddebniak, C. Dresen, J. Müller, F. Ising, S. Schinzel, S. Friedberger, J. Somorovsky, J. Schwenk, "Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels", August 2018, https://www.usenix.org/conference/usenixsecurity18/presentation/poddebniak

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

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

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

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

15. 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.

16. Appendix A: File Formats Considered

The following file formats were considered in the development of this specification. Some were selected while others were left out.

16.1 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.

Certain older cipher suites utilizing the CFB mode of operation are vulnerable to attack [EFAIL]. This specification requires the use of modern cipher suites using Authenticated Encryption with Associated Data (AEAD).

16.2 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.

Unfortunately, S/MIME is vulnerable to several known CBC attacks [EFAIL] and (unlike OpenPGP) there are no available mitigations at the time this specification was written.

16.3 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.

17. Change History

17.1 April 18, 2019

- Updated to use specification template (now standards-track).
- Changed Registration to Specification throughout
- Changed encrypted Job to Encrypted Job throughout
- Section 2.4: Added Encrypted Job, Job Receipt, and Job Ticket terms.
- Section 6.3: Only the originator and admins/operators can access the encrypted job attributes
- Section 7.1.3: Base64 key block, application/ipp+pgp-encrypted mime type
- Section 7.2.2: Base64 key block
- Section 8.1: Added the requesting-user-pgp-public-key operation attribute to the attributes that are included in the encrypted IPP message passed in Print-Job and Send-Document requests.
- Section 11, 14.2: Drop XML Unicode TR
- Section 12: Added considerations for the PGP cipher suite used (AEAD)
- Section 13: Updated IANA stuff
- Section 14: Updated references

17.2 January 31, 2019

- Dropped S/MIME due to EFAIL vulnerabilities
- Added reference to EFAIL presentation and paper
- Added use case for retrieving an encrypted job receipt
- Added Acknowledge-Encrypted-Job-Attributes, Fetch-Encrypted-Job-Attributes, and Get-Encrypted-Job-Attributes operations
- Added 'encrypted-job-attributes-requested' printer state reason keyword.
- Updated all references as needed.

17.3 March 28, 2018

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

17.4 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).

17.5 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.

17.6 February 4, 2015

Initial revision, presented at PWG February 2015 F2F.

