The Printer Working Group

February 5, 2018
White Paper

IPP Document Encryption (DOCCRYPT)

Status: Initial

Abstract: This document is a whitepaper that defines a new IPP convention for encrypting document content to provide IPP with end-to-end encryption of Document content, including an encoding convention and a set of IPP attributes to convey metadata about the encoding system being used.

This document is a White Paper. For a definition of a "White Paper", see: http://ftp.pwg.org/pub/pwg/general/pwg-process30.pdf

This document is available electronically at:

http://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-doccrypt-20180205.odt
http://ftp.pwg.org/pub/pwg/ipp/whitepaper/tb-doccrypt-20180205.pdf

Title: IPP Document Encryption *(DOCCRYPT)*

Table of Contents

List of Figures

List of Tables

1 Introduction

While IPPS [RFC7472] can provide transport confidentiality, in some cases it is important to the User to provide so-called “end-to-end encryption”, where the Document content is to be encrypted before it is submitted to the Printer, and remain encrypted until the encryption credential is provided to decrypt it. This specification defines a system for IPP Document Data encryption as well as a set of IPP attributes that convey metadata describing attributes of the encoding system being used.

2 Terminology

2.1 Protocol Roles Terminology

This document defines the following protocol roles in order to specify unambiguous conformance requirements:

Client: Initiator of outgoing IPP session requests and sender of outgoing IPP operation requests (Hypertext Transfer Protocol -- HTTP/1.1 [RFC7230] User Agent).

Printer: Listener for incoming IPP session requests and receiver of incoming IPP operation requests (Hypertext Transfer Protocol -- HTTP/1.1 [RFC7230] Server) that represents one or more Physical Devices or a Logical Device.

Secure Print: An IPP feature described in [PWG5100.11] to restrain Job processing until a Job password has been provided to the Printer.

Encrypted Document: A Document submitted as part of a job that is encrypted according to a particular encryption scheme, in order to provide confidentiality of the document content while the Document is in a pre-processing state.

2.2 Other Terms Used in This Document

User: A person or automata using a Client to communicate with a Printer.

2.3 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 Rationale for IPP Document Encryption

Existing specifications define the following:

1. The Internet Printing Protocol/1.1: Model and Semantics [RFC8011] defines "document-format" Job Template attribute.

2. "Internet Printing Protocol (IPP) over HTTPS Transport Binding and the 'ipps' URI Scheme" [RFC7472] defines the IPP over HTTPS transport binding. HTTPS provides session transport encryption. HTTP includes semantics for a Server to challenge a Client for authentication credentials when establishing a connection.

This whitepaper defines a new IPP convention for encrypting document content to provide the IPP ecosystem with a mechanism to provide end-to-end encryption of Document content by:

1. Specifying a set of standard encryption types

2. Creating new IPP Printer Description attributes that convey information about the encryption / decryption capabilities of the Printer

3. Creating new IPP Job Template attributes that convey information about the encryption choices used by the Client to encrypt the Document content

3.1 Use Cases

The following use case descriptions illustrate the needs that this specification proposes to solve.

3.1.1 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 IPP Encrypted Document, and encryption schemes supported by both his Client and the Printer, which are discovered and confirmed in the discovery process.

Garrett makes his job choices, including selecting IPP Encrypted Document and providing an authentication credential, and taps "Print" to submit his choices. The Client encrypts the 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.

3.1.2 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 authenticates with the cloud print service, chooses the Document or the Job containing the Document and taps “Print”. The Document arrives at the Printer, still encrypted. 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.

3.1.3 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.

3.1.4 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

3.1.5 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.

3.2 Exceptions

3.2.1 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 Output Device. The Printer notifies Garrett that the document has been changed. Garrett chooses to abandon the output.

3.3 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
2. The method and apparatus used by the Printer to receive the credential (e.g. password or certificate public key) needed to decrypt the encrypted document

3.4 Design Requirements

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

1. Selecting one or more document formats that support the following criteria:
    a. An encrypted payload
    b. Digital signature(s)
    c. Metadata describing the document format itself, as well as other information such as parameters used for the document encryption
    d. An evolving set of encryption parameters algorithms, hash algorithms, etc. that don't need to be designed or maintained by the PWG.
    e. Can evolve to align with current best practices and state of the art techniques without having to respecify new formats
2. Selecting one of the above document formats to be the baseline format that all printers supporting IPP Document Encryption must support, to ensure baseline interoperability.
3. Replicating pertinent document metadata via IPP attributes to allow IPP operations to retrieve the metadata without retrieving the document itself.

4. Support for both symmetric and asymmetric encryption systems.
5. Ensuring that IPP can convey a normalized set of document encryption options using IPP attributes.
6. Register all attributes and operations with IANA and the PWG

The following design recommendations should be met by solutions specified in this document:

1. Outlining a best-practice user experience

4 Overview

Users take it for granted that their print jobs will be confidential and that they will have control of them when they are printed. When IPPS is used, transport encryption and authentication can be enforced. But if there are multiple stages between the Client and the Output Device, then there can be connections that are not confidential. Additionally, the user should have an option to encrypt their job end-to-end, so that intermediate elements do not have the opportunity to change or examine the content without the originating user's control.

5 Printer Description Attributes

5.1 document-encryption-cipher-default (type2 keyword)

The “document-encryption-cipher-default” attribute specifies the cipher preferred by the Printer. This attribute MUST be implemented if “document-encryption-ciphers-supported” is implemented. The value specified by “document-encryption-cipher-default” MUST be one of the values found in “document-encryption-ciphers-supported”.

5.2 document-encryption-ciphers-supported (1setOf type2 keyword)

The “document-encryption-ciphers-supported” attribute specifies the set of ciphers supported by the Printer. This attribute MUST be implemented if “document-encryption-cipher-default” is implemented.

5.3 document-encryption-credential-type-default (type2 keyword)

The “document-encryption-credential-type-default” attribute

5.4 document-encryption-credential-type-supported (1setOf type2 keyword)

The “document-encryption-credential-type-supported” attribute

6 Document Template Attributes

6.1 document-encryption-cipher (type2 keyword)

The “document-encryption-cipher” attribute specifies the cipher used to encrypt the Document. This is used along with the credential to properly decrypt the Document for processing.

6.2 document-encryption-credential-type (type2 keyword)

The “document-encryption-credential” attribute specifies the credential type expected to be requested of the User when the Document is to be decrypted for processing.

7 IPP Document Encryption Process

Document content format information is conveyed in IPP using the "document-format" attribute [RFC8011]. To allow signed and/or encrypted document content to be carried by IPP, the Document is encoded into the "multipart/encrypted" MIME Media Type [RFC1847]. The "document-format" attribute specifies that media type in the IPP operation used to transmit the document content.

8 Internationalization Considerations

For interoperability and basic support for multiple languages, implementations use the Universal Character Set (UCS) Transformation Format -- 8 bit (UTF-8) [RFC3629] encoding of Unicode [UNICODE] [ISO10646] and the Unicode Format for Network Interchange [RFC5198].

9 Security Considerations

Provide security considerations for this document.

10 IANA and PWG Considerations

10.1 Attribute Registrations

The attributes defined in this document will be published by IANA according to the procedures in IPP Model and Semantics [RFC8011] section 6.2 in the following file:

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

The registry entries will contain the following information:


```
Job Template attributes:                                    Reference
-------------------------                                   ------------
finishings-col (no-value | 1setOf collection)               [PWG5100.1]
```

11 References

[http-encryption] M. Thomson, "Encrypted Content-Encoding for HTTP (draft-ietf-httpbis-encryption-encoding-08)", Internet-Draft, March 2, 2017, https://tools.ietf.org/html/draft-ietf-httpbis-encryption-encoding-08

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

[PWG5100.11] T. Hastings, D. Fullman, "IPP: Job and Printer Operations - Set 2", PWG 5100.11-2010, October 2010, http://ftp.pwg.org/pub/pwg/candidates/cs-ippjobprinterext10-20101030-5100.11.pdf

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

[PWG5100.19] S. Kennedy, "IPP Implementor's Guide v2.0", PWG 5100.19-2015, August 2015, http://ftp.pwg.org/pub/pwg/candidates/cs-ippig20-20150821-5100.19.pdf

[RFC1847] J. Galvin, S. Murphy, S. Crocker, N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC 1847, October 1995, http://www.ietf.org/rfc/rfc1847.txt

[RFC2817] R. Khare, S. Lawrence, “Upgrading to TLS Within HTTP/1.1”, RFC 2817, May 2000, https://www.ietf.org/rfc/rfc2817.txt

[RFC3629] F. Yergeau, “UTF-8, a transformation format of ISO 10646”, RFC 3629, November 2003, https://www.ietf.org/rfc/rfc3629.txt

[RFC5198] J. Klensin, M. Padlipsky, “Unicode Format for Network Interchange”, RFC 5198, March 2008, https://www.ietf.org/rfc/rfc5198.txt

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

[RFC7472] I. McDonald, M. Sweet, “Internet Printing Protocol (IPP) over HTTPS Transport Binding and the 'ipps' URI Scheme”, RFC 7472, March 2015, https://tools.ietf.org/html/rfc7472

[RFC8010] M. Sweet, I. McDonald, “Internet Printing Protocol/1.1: Encoding and Transport”, RFC 8010, January 2017, https://www.ietf.org/rfc/rfc8010.txt

[RFC8011] M. Sweet, I. McDonald, “Internet Printing Protocol/1.1: Model and Semantics”, RFC 8011, January 2017, https://www.ietf.org/rfc/rfc8011.txt

[UNICODE] The Unicode Consortium, “The Unicode Standard, Version 6.2.0”, ISBN 978-1-936213-07-8, September 2012, http://www.unicode.org/versions/Unicode6.2.0/

12 Authors' Addresses

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

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

Turanga Leela - Planet Express
Zapp Brannigan - Democratic Order of Planets
Ira McDonald – High North, Inc.
Mike Sweet – Apple Inc.

13 Change History

13.1 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.

13.2 February 4, 2015

Initial revision, presented at PWG February 2015 F2F.

