PWG®

The Printer Working Group

IPP Document Encryption Topics

February 7, 2018

Copyright © 2018 The Printer Working Group. All rights reserved. The IPP Everywhere and PWG logos are trademarks of the IEEE-ISTO.

Overview/History

- Currently IPP offers very limited support for document encryption:
  - In transit: TLS
  - At rest: Passphrases passed in the Job/Document Creation Request ("document-password"), used to "unlock" an encrypted PDF, OpenXPS, etc. file
- No support for encryption of documents using credentials that are not passed to the Printer/intermediary handling the Job/Document Creation Request
  - Important for cloud/infrastructure printing use case
- No support for encryption/protection of saved documents
  - See "IPP Job Save Password" proposal

Copyright © 2018 The Printer Working Group. All rights reserved. The IPP Everywhere and PWG logos are trademarks of the IEEE-ISTO.

Existing Solutions

- Various ZIP archive features:
  - Password-based encryption (insecure)
  - Public key crypto (not widely implemented, platform interop issues)
- OpenPGP
  - Multiple interoperable implementations
  - Various extensions for use with email, etc.
  - Encrypt whole document or just a symmetric key using the public key
  - Digital signatures and passphrases, too.
- Others?

Copyright © 2018 The Printer Working Group. All rights reserved. The IPP Everywhere and PWG logos are trademarks of the IEEE-ISTO.

Use Cases

- Protection from intermediaries: submit an encrypted Document for printing that is passed through to the final output device without processing/transforms
- Protection from alteration: submit a digitally signed Document for printing; the attached signature can be validated by the intermediaries and final output device prior to processing/transforms
- Secure PIN printing: submit an encrypted Document using a passphrase for printing that is not processed/transformed until the User enters the passphrase at the console
  - (Passphrase is used in the encryption of the Document, not just passed in the Job Creation Request)

Copyright © 2018 The Printer Working Group. All rights reserved. The IPP Everywhere and PWG logos are trademarks of the IEEE-ISTO.

Requirements

- Printer needs to advertise support
  - If PGP, public key and whether passphrases are supported (and what the repetoire is)
  - Should encryption be supported for all other advertised formats, i.e., a Printer supports any format in encrypted form? Or do we want a parallel list of supported encrypted formats?
- Client needs to use the encryption info/capabilities from the Printer, somehow tell the Printer the actual format
- Need a MIME media type
  - multipart/encrypted is not suitable for IPP
  - For PGP, application/pgp-encrypted is just a placeholder followed by an application/octet-stream part containing the encrypted message
  - So maybe define an "application/ipp-encrypted-document" media type?
- Support digital signatures embedded in encrypted document

Copyright © 2018 The Printer Working Group. All rights reserved. The IPP Everywhere and PWG logos are trademarks of the IEEE-ISTO.

Possible Solution ("IPP Encrypted Jobs and Documents")

- Adopt OpenPGP (RFC 4880)
- New Printer Description attributes:
  - "pgp-document-format-supported (1setOf mimeMediaType)"
    - List of document formats that can be PGP-encrypted
  - "printer-pgp-public-key (1setOf text(MAX))"
    - PGP public key to use when encrypting documents, can be set by Proxy in infrastructure printing
  - "printer-pgp-repertoire-configured (type2 keyword)"
  - "printer-pgp-repertoire-supported (1setOf type2 keyword)"
    - Provided if additional passphrase is supported at console (to release for printing)
- New MIME Media Type "application/ipp-pgp-encrypted"
  - PGP-encrypted IPP message containing Job/Document ticket followed by Document data

Copyright © 2018 The Printer Working Group. All rights reserved. The IPP Everywhere and PWG logos are trademarks of the IEEE-ISTO.

Security Considerations

- Need to validate embedded digital signatures and refuse to print if the signature has been altered
  - New "job-state-reasons" value
- Need to validate public key advertised by Printer
  - If a malicious intermediary provides its own public key then it could decrypt the document

Copyright © 2018 The Printer Working Group. All rights reserved. The IPP Everywhere and PWG logos are trademarks of the IEEE-ISTO.