

Trilateral Technical Standard for the On-line Exchange of IP Documents in a PKI Environment

1	BACKGROUND	2
2	SCOPE	2
3	SECURITY	2
3.1	PUBLIC KEY INFRASTRUCTURE	2
3.2	CERTIFICATES	3
3.3	CERTIFICATION AUTHORITIES	4
3.4	CERTIFICATION MANAGEMENT	4
3.5	CROSS CERTIFICATION	7
3.6	DIGITAL SIGNATURES	7
3.7	DIRECTORY SERVICES	8
3.8	ENCRYPTION ALGORITHMS	8
3.9	DATA ENCRYPTION	8
3.10	STRONG ONE-WAY MESSAGE DIGEST ALGORITHMS	8
3.11	SECURITY AND PAYMENT MECHANISMS	8
3.12	SUMMARY OF SECURITY MECHANISMS	8
4	SIGNATURES MECHANISMS	9
4.1	BASIC ELECTRONIC SIGNATURE	9
4.2	ENHANCED ELECTRONIC SIGNATURE	9
5	DOCUMENT PACKAGING	10
5.1	DOCUMENT PREPARATION	10
5.2	WRAPPING THE DOCUMENTS	10
5.3	SIGNING THE WRAPPED DOCUMENTS	11
5.4	PACKAGING THE WRAPPED AND SIGNED DOCUMENTS	11
6	SUBMISSION	12
6.1	TRANSFER PROTOCOL	14
7	TYPES OF DOCUMENT EXCHANGE	14
8	REFERENCE IMPLEMENTATIONS	14
	ATTACHMENT 1. DOCUMENT FORMAT REQUIREMENTS	15
	ATTACHMENT 2. WRAPPING SPECIFICATION (SDIF V2)	16
	ATTACHMENT 3. PKCS#7 ENVELOPE FORMATS	18
	ATTACHMENT 4. TICKET MECHANISM	22
	ATTACHMENT 5. RECORDS MANAGEMENT REQUIREMENTS	27
	ATTACHMENT 6. ACRONYMS	30

1 Background

This document presents the technical requirements for on-line filing in a PKI environment. This standard is expected to evolve to cover all types of exchange of Intellectual Property Documents including the PCT procedure as well as non-patent procedures such as trademarks. Text in square brackets “[]” indicates requirements that are recommended to become part of the standard in future.

This standard represents a maximum set of measures that an IP Office can require of an applicant.

It has been adopted by the Trilateral Offices as the standard for the implementation of on-line filing pilots and for interoperability testing.

2 Scope

This specification allows all types of IP documents (Patents, Trademarks, Utility Models etc) to use the same mechanisms for electronic communication between applicants, Receiving Offices, Authorities and the IB for PCT as well as National Procedures.

The technical implementation for different types of exchange rely on the following aspects:

- Security and PKI
- Electronic Signatures
- Document Packaging
- Submission

3 Security

This section addresses requirements for:

1. the security of electronic documents that are transmitted over communication networks in the course of conducting electronic commerce with Intellectual Property (IP) Offices, and
2. the security of electronic documents held by IP offices subject to electronic record management practices. In particular, this covers the mechanisms needed to protect computer systems at IP Offices against unauthorised penetration.

After the requirements are identified, the section specifies technical standards to be used when implementing systems to fulfil the requirements.

Security requirements for the exchange and storage of IP electronic documents are derived from treaty and law protecting the content of IP electronic documents from inappropriate disclosure and the need to support the validity, admissibility and weight of IP electronic documents in legal proceedings. Consequently, IP office automation and electronic filing systems must reliably preserve the confidentiality and integrity of IP electronic documents while implementing features to ensure originator authentication and non-repudiation. Concise definitions of these qualities follow.

3.1 Public Key Infrastructure

Public Key cryptography techniques supply most of the accepted methods and defacto standards for providing these qualities in Internet electronic commerce. In public key cryptography key pairs are created. The key pairs have the property that each key of a pair can be used to decrypt data that was encrypted using the other key. Users of Public Key

cryptographic systems publish one key from the pair (the public key) and protect the other key from disclosure (the private key). Public Key cryptography is supplemented by the use of strong one-way message digest functions to establish the integrity of electronic documents. The two technologies are used to create digital signatures. To make a digital signature a message is input to a strong one-way message digest function and the result of the function, called a message digest, is encrypted using the private key.

Digital certificates have been developed as a means to bind the identity of parties with their public key. A digital certificate is a compact data message bearing the identity of its owner, the owner's public key and a means of independently verifying that the certificate can be trusted. Digital certificates may be issued either by one of the parties to the electronic business transaction after establishing the identity of the other party, or by a trusted third party. In the third party case, both parties to the electronic business transaction trust the policies and practices used by the third party to establish identities. For digital certificates to be useful it must be possible to revoke them when they are no longer valid. Situations leading to certificate cancellation include:

- a compromise of the private key paired with the public key on the certificate,
- the address or other identity information changes,
- a mistake is discovered in the certificate,
- an affiliation (such as employer) of the holder changes or
- the expiration date of a certificate is past.

To provide comprehensive security on a large scale, large numbers of digital certificates are required. An organization such as an IP office that desires to conduct bi-directional electronic commerce on the Internet with its customers protected by confidentiality, integrity, authentication and non-repudiation features needs to recognize a digital certificate for each customer. The policies and procedures plus the suite of systems and software required to issue, revoke, retrieve and manage large numbers of digital certificates is called a Public Key Infrastructure (PKI).

A PKI includes the following components:

Registration Authority (RA)	interacts with parties requesting a certificate to establish identities
Certification Authority (CA)	issues certificates based on applications received from the RA
Certificate Management	handles certificate renewal, revocation for expiration, revocation for cause, distributes Certificate Revocation List (CRL), validates certificates, validates digital signatures, provides API for use by software applications
Directory Service	maintains database of certificates and retrieves certificates for use
Certification Policies and Practices Statement	documents the operational practices and rules under which the PKI operates

3.2 Certificates

All digital certificates used in IP Document Exchange shall comply with the International Telecommunication Union (ITU) X.509 Version 3 Recommendation for certificate format. See: Recommendation X.509 (08/97) – Information technology – Open Systems Interconnection – The Directory: Authentication framework.

Requests for digital certificates shall be prepared in compliance with the PKCS#10 Standard. See: RSA Laboratories, PKCS #10 – Certification Request Syntax Standard Ver. 1

Certificates may be issued as follows:

- On Smart Cards
- On Diskette
- On-line

Public Key Infrastructure (PKI) systems shall interoperate based on use of the X.509 Version 3 Certificates and X.509 Version 2 Certificate Revocation Lists . Implementations of PKI systems shall comply with the recommendations established by the Internet Engineering Task Force (IETF) Working Group on PKI Interoperability (PKIX) and documented in IETF RFC 2459. Draft standards documents are available from the University of Southern California Information Sciences Institute at <ftp://ftp.isi.edu/internet-drafts/>. See the following draft standards documents:

<i>Internet Draft Filename</i>	<i>Title of Specification</i>
draft-ietf-pkix-ipki3cmp	Internet X.509 Public Key Infrastructure Certificate Management Protocols
draft-ietf-pkix-crmf	Certificate Request Message Format
draft-ietf-pkix-ipki-part4	Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices framework
draft-ietf-pkix-ipki-part1	Internet Public Key Infrastructure X.509 Certificate and CRL Profile
draft-ietf-pkix-ldapv2-schema	Internet X.509 Public Key Infrastructure LDAPv2 Schema

Implementations of PKI systems shall use separate key pairs and digital certificates for the purpose of authentication and confidentiality. The authentication keys shall be the property of the IP office customer, and the private key of the authentication keypair shall never leave the IP office customer's custody.

An IP Office may decide to offer Key Recovery for the security keypair when allowed under national laws.

3.3 Certification Authorities

Certification Authorities are responsible for maintaining the accuracy of the electronic certificates that “prove” a party is who he says he is. There can be many such authorities. Certificates will be issued as determined by each CA according to national law.

[The IB maintains a list of root Certification Authorities for the International IP community. The Offices will select from this list those root authorities that they will accept for certificate validation. The IB may also act as a CA.]

Each IP Office will subscribe to Certificate Revocation Lists for all CAs that it accepts. Whenever a certificate is used to authenticate an individual, these Certificate Revocation lists will be consulted by the IP OFFICE to ensure that the certificate has not been revoked.

3.4 Certification Management

The process of issuing, managing, and revoking certificates is divided into eight parts, referred to as the Certificate Life Cycle. The major life cycle processes are:

- Certificate Application

- Validation of Certificate Application
- Certificate Generation, Issuance, and Distribution
- Acceptance of Certificate by Subscriber
- Certificate Use
- Certificate Expiration and Renewal
- Certificate Revocation
- Key Recovery

Each of these processes has its own set of policies and procedures that will be followed, assuring that the PKI will provide a trusted environment. The first three phases are directed towards assuring that certificates are issued to appropriate individuals. The fourth and fifth phases refer to usage of the certificate by a certificate holder (called a subscriber). The last three phases address the end of the life cycle, where a certificate expires naturally, or a certificate may be revoked and replaced with a new one.

3.4.1 Certificate Application

This phase is the beginning of communication between subscriber and Certification Authority and thus initiates the certificate life cycle. IP Office personnel will not have to complete a certificate application. Employee status will provide the required evidence of identity and need for these certificates. Others will normally apply for a certificate by completing and submitting a certificate application that provides specific subscriber information, including name, organization, and certificate type. Written applications may be required initially; however, future enhancements to the PKI will implement on-line certificate applications. An external requester will be required to complete a subscriber agreement that sets out his obligations regarding the use of the certificate issued to him.

3.4.2 Validation of Certificate Application

The Registration Authority has responsibility for authenticating the identity of the certificate subscriber and affirming the accuracy of information submitted, including the need for the certificate. After validation of information in the certificate application, the Registration Authority authorizes the creation of certificates by the Certification Authority for the subscriber. The Certification Authority validates the authorization from the Registration Authority, to make sure that the authorization was issued by a valid Registration Authority and that it contains all of the required information. The Certification Authority then provides the subscriber with the information necessary to complete the certificate issuance process. The identity proofing function may be delegated to a Local Registration Authority (LRA) with organizational or customer focus. Certificate validation is closely tied to certificate application.

3.4.3 Certificate Generation, Issuance and Distribution

The subscriber uses PKI client software to complete a series of steps that results in the creation of key pairs, and the generation, issuance and distribution of public key certificates. Two key pairs (four keys) are created in the process: one encryption key pair and one signing key pair. The encryption key pair consists of the encryption public key and decryption private key. When created, the encryption public key is automatically sent to the Certification Authority platform where it is entered in a public key certificate and signed by the Certification Authority. The signing key pair consists of a signing private key and a verification public key. The verification public key is automatically sent to the Certification Authority where it is entered in a public key certificate and signed by the Certification Authority. If key recovery is implemented, a copy of the private decryption key is stored in a key recovery system for use if the decryption key becomes unavailable. The Certification Authority posts the encryption public key certificate to the appropriate Directory (certificate repository) and returns the verification public key certificate to the subscriber's PKI client software.

3.4.4 Acceptance of Certificate by Subscriber

The external subscriber can indicate acceptance of the certificate by various means such as by written agreement, or by use of the certificate to send a signed message to the Registration Authority acknowledging receipt of the certificate, or by use of the certificate to establish an encrypted session.

3.4.5 Use of Certificate

Subscribers encrypt objects (e.g., files, forms, documents, email) for intended recipients by using the recipient's public encryption key obtained from their encryption public key certificate; only the intended recipient is able to decrypt the object using his/her private decryption key.

Subscribers digitally sign objects using their private keys. Relying parties can verify the signatures of subscribers and the integrity of the signed object by obtaining the signer's public verification key from their verification public key certificate, which is provided with the signed object, and using it to verify the digital signature.

In both cases, the public key certificate and current certification revocation list are obtained by the relying party's PKI client software. The PKI client software then verifies the Certification Authority's signature on the certificate and from the Certificate Revocation List, verifies that the certificate has not been revoked, and in the case of digital signature verification, that the signature verification certificate was valid when the digital signature was executed. These activities are accomplished via simple icon or pop down menu choices executed by the user. This process will be automated.

3.4.6 Certificate Expiration and Renewal

Each certificate has a set life span after which it expires and needs to be renewed. The life span is set to avoid vulnerabilities that may occur if an attacker has a large collection of messages signed or encrypted with the same key and sets about breaking the key, a time intensive process. Normally, internal subscribers' certificates will be automatically renewed before they expire, with new key pairs generated and certificates issued. External subscribers may be required to request renewal. External subscriber software notifies the end user of pending expiration.

When key pairs are updated, they are replaced with new key pairs and new public key certificates are created. If a subscriber's certificate requires update for other than normal time expiration reasons, the subscriber and Registration Authority will need to be involved. Such reasons include the need to modify subscriber identification information, policy that requires periodic confirmation of subscriber information, or to resolve suspected misuse or key compromise.

3.4.7 Certificate Revocation

A subscriber's certificate may be revoked for any of several reasons. Certificate revocation may be initiated by the subscriber, the Registration Authority or Local Registration Authority, and/or authorized IP Office management. Subscribers should advise the cognizant Registration Authority or Local Registration Authority if they 1) no longer require use of the certificate (e.g., termination of employment, change of job responsibilities), 2) know of or suspect a compromise of their private key, or 3) have changed their name. In the absence of a request by the subscriber, the cognizant Registration Authority or Local Registration Authority should request revocation of a subscriber's certificate for any of the above reasons. The cognizant Registration Authority or Local Registration Authority should also initiate revocation of a subscriber's certificate if there is a material breach of the subscriber agreement.

3.4.8 Key Recovery

A subscriber should be able to recover data, which they have encrypted or that was encrypted for them, even though their decryption private key becomes unavailable. The key may become

unavailable for a variety of reasons including, inability to access the stored key (e.g., forgets password), corruption of the stored key, failure of the storage medium, and theft of the key or storage medium. An organization should be able to recover its data, which has been encrypted by subscribers, when the subscriber is unable or unwilling (e.g., disgruntled, incapacitated, unavailable) to decrypt the data.

The IP Office PKI may provide the capability for key recovery of internal and external subscriber decryption keys. In order to meet these requirements, a copy of each user's private decryption keys must be obtained and securely stored to enable the authorized recovery of encrypted data.

Key recovery does not apply to the subscriber's signing keys. The subscriber's private signing keys are not recoverable due to the requirement for effective non-repudiation. Non-repudiation is supported by having the subscriber generate his signing key pair on his own system and only transferring his public verification key to the Certification Authority during the registration process. The private signing key must remain under the sole control of the subscriber so that there is no opportunity to masquerade.

The following discussion applies to decryption key recovery only. It is a highly sensitive PKI function since it deals with the confidentiality of communications and files which may, as with patent application prosecution, be held in confidence by law.

Key recovery for external subscribers may only be initiated by the subscriber, a Registration Authority, or a Local Registration Authority by following established key recovery procedures and interacting with the Registration Authority.

For internal subscribers, a Registration Authority or Local Registration Authority should initiate key recovery only after authorization by appropriate IP office management. Such authorization may result from a request from the internal subscriber or from a requirement by management to access data encrypted by the subscriber.

3.5 Cross Certification

The Trilateral Offices have indicated that they will maintain their own Certificate Authorities. As a result, there are likely to be several root certificates in IP Document Exchange. Cross certification provides a method to greatly reduce the need to distribution root certificates throughout the system and a resulting simplification of root certificate management.

When two communities of users each have a Certification Authority, a process called cross certification can be used so that the users of one community can trust the public key certificates of the users in the other community, and visa versa. This is accomplished by having the two Certificate Authorities issue certificates for each other's public key. User PKI client software can process these certificates to determine whether the public key certificate of a user in another community should be trusted. It is important that a determination is made that the certificate policies of each community of users are at equivalent levels of assurance. The questions and issues arising related to accepting policies between offices will be more challenging than the technical issues of providing cross certificates.

For the present, until a model Certificate Policy can be accepted by the various IP Offices, cross certification will be accomplished on a case-by-case basis, based on a successful review of the parties respective Certificate Policies. In addition, some third party certification authority, as yet unidentified, can be requested by the Office to certify compliance with the published described procedures, which certification would also be published.

3.6 Digital Signatures

Digital signatures used to sign electronic documents for IP Document Exchange shall conform to the format and practice specified in RSA Laboratories, PKCS #7 – Cryptographic Message

Syntax Standard Version 1.5 definition of Signed-data content type. To build these signatures, a certificate is needed. These are X.509 version 3 certificates signed by an approved Certification Authority (CA).

3.7 Directory Services

All Offices participating in electronic document exchange must subscribe to the CRLs described above and must use these when decoding a PKCS#7 package.

PKI Systems shall store certificate information in a directory structure complying with ITU Recommendation X.500. Such systems shall provide an external interface for publishing and retrieving user digital certificates that complies with the Lightweight Directory Access Protocol (LDAP). See IETF Network Working Group RFC 1777 dated March 1995.

3.8 Encryption Algorithms

Both symmetric (secret key) and asymmetric (public key) algorithms may be used as necessary. Algorithms that are prohibited under national law of a country shall not be used for IP Document Exchange from that country. Algorithms implemented in hardware or software shall not be used in any manner that is contrary to export restrictions of the country of origin for the hardware or software. Any algorithm used between IP Offices must be disclosed to both parties.

3.9 Data Encryption

Electronic document data that is encrypted to ensure confidentiality for IP Document Exchange shall conform to the format and practice specified in RSA Laboratories, PKCS #7 – Cryptographic Message Syntax Standard Version 1.5 definition of Signed and Enveloped-data content type.

3.10 Strong One-Way Message digest Algorithms

The message stream shall be input to a strong one-way message digest algorithm to create a message digest. The one-way message digest algorithm shall be SHA-1.

3.11 Security and Payment Mechanisms

The security offered under the PKI system for data confidentiality shall also be deemed sufficient to protect the confidentiality of Credit Card information transmitted online for fees or other payments.

3.12 Summary of Security mechanisms

The following table shows how, in a PKI environment, various technical components meet the Confidentiality, Integrity, Authenticity and Non-repudiation:

	Confidentiality	Integrity	Authenticity	Non-repudiation
Certification Authority			X	X
Digital Certificates		X	X	X
Certification Management		X	X	X
Cross Certification		X	X	X
PKCS#7 Signed Data Type		X	X	X
Directory Services			X	X
Encryption Algorithms	X			
PKCS#7 Signed and Enveloped Data Type	X			

	Confidentiality	Integrity	Authenticity	Non-repudiation
Message digest Algorithm		X		
PKI Policy Statements		X	X	X

4 Signatures Mechanisms

A signature functions in the electronic world to identify a particular person as a source of the electronic message. It also indicates such a person's approval of the information contained in the electronic message.

For the purposes of this document, there are two signature mechanisms:

- Basic Electronic Signature
- Enhanced Electronic Signature

This signature, which includes the full name of the signature holder as well as place and date of signature, is embedded in the document as XML tagged data (See Appendix II for the XML DTD). The XML tagged data either indicates that the user wishes to apply their Enhanced Electronic Signature to the electronic message or their Basic Electronic Signature.

4.1 Basic Electronic Signature

To indicate the human intention to perform a certain action, the standard includes the specification of a basic electronic signature. This is can be one of the following types of signature:

- A particular string of text entered by a user
- A facsimile image of the handwritten signature

The Basic Electronic Signature is encoded within the "party" structure of the XML document shown below:

```

...
<!ELEMENT electronic-signature
      (date-signed,
       place-signed,
       ((signature-mark,signature-file?)
        | (signature-file,signature-mark?)
        | use-digital-signature)) >
...

```

A Basic Electronic Signature within an XML document may be supplemented by the addition of a Digital Signature of the Signer's Representative to the Wrapped Documents.

4.2 Enhanced Electronic Signature

This is a PKCS#7 Signed Data Type generated from the electronic message by the act of the signer invoking the use of their private authentication key to encrypt the message digest (Digital Signature). The PKCS#7 Signed Data Type includes a copy of the Digital Certificate of the signer issued by a recognised Certification Authority.

5 Document Packaging

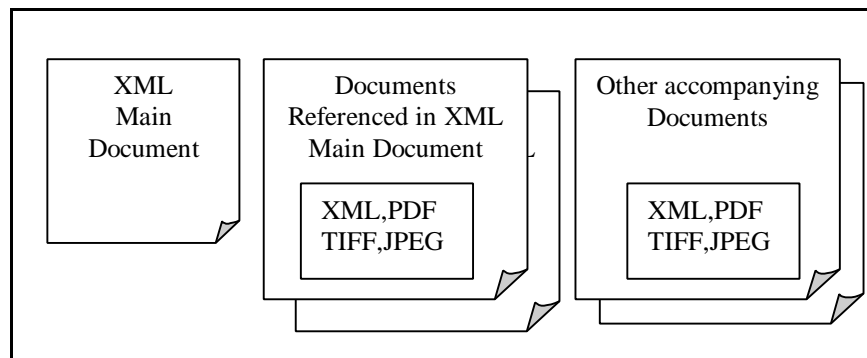
The document packaging mechanism is used to combine into a single binary object both the data about what is being transmitted with the contents of the transmission and to then apply the appropriate digital signatures and encryption.

5.1 Document Preparation

For each IP Document Exchange there is an XML Main Document that may explicitly reference and be hyper-linked to other documents. These referenced documents are logically part of the Main Document (e.g. a New Patent Application). In addition, a document exchange may include other accompanying documents (e.g. Designation of Inventor or a Fee Payment).

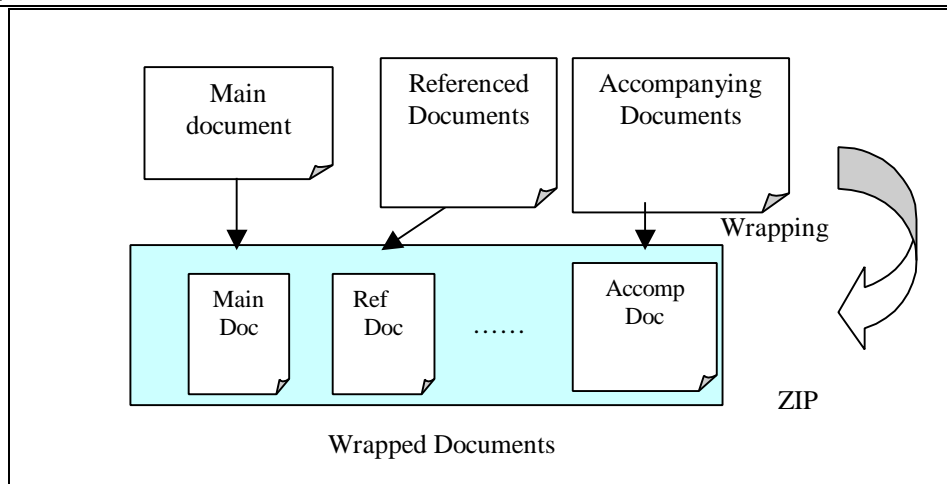
The XML Main Document must conform to one of the DTDs specified in Appendix II. The Referenced Documents (external entities) are typically embedded images, tables, drawings or other compound documents and may be encoded as either XML, PDF, TIFF and JPEG. See Attachment 1 for details.

The accompanying documents are separate, but related documents that may be encoded as either XML, PDF or Image. See Attachment 1 for details.



5.2 Wrapping the Documents

The Main Document with any Externally Referenced Documents and Accompanying Documents are wrapped and treated as one data block. This data block is called the Wrapped Documents and is created using the wrapping standard (ZIP). Applicants shall use ZIP format archiving and compression software to package the document files constituting an electronic application. The software used to create the ZIP file shall conform to the ZIP format standard as published in the PKWARE® PKZIP® Application Note. National Offices, WIPO and Third party vendors and implementers of filing software shall verify that any ZIP software used complies with the Application Note standard. Attachment 2 describes the ZIP standard in detail.

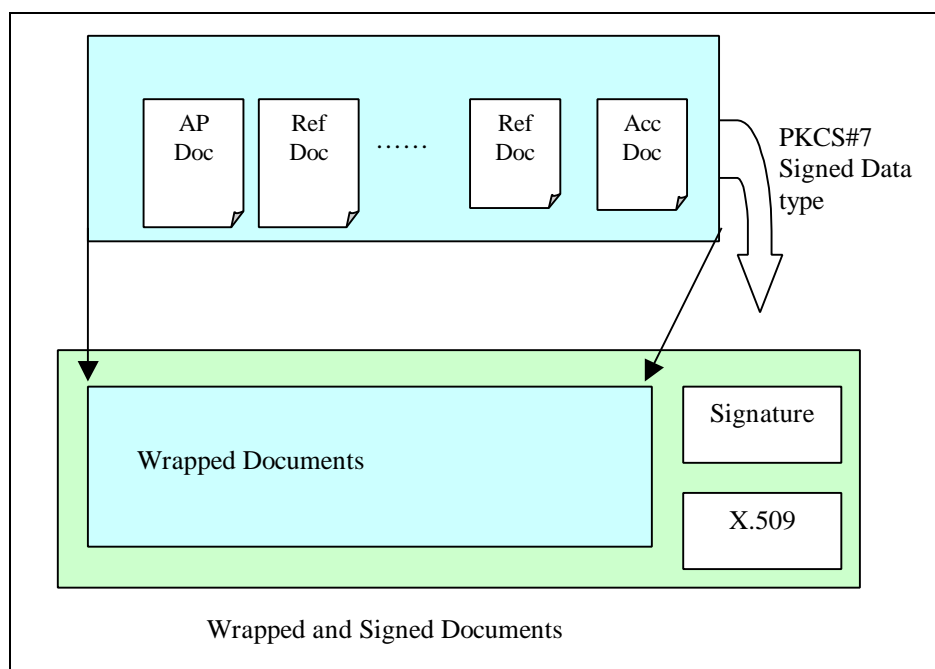


See Attachment 1 for details of the allowed document format types.

5.3 Signing the Wrapped Documents

To bind the person submitting the package to the electronic Wrapped Documents, a Digital Signature is added to create the Wrapped and Signed Document Data item. The purpose of adding the signature is to identify the applicant and to ensure that the recipient is able to detect any unauthorized alternation during the transmission.

PKCS#7 is used to produce a Signed Data Type for the signature. Detailed information on PKCS#7 is provided in Attachment 3.



5.4 Packaging the Wrapped and Signed Documents

A package is the actual transmission data that is exchanged between the applicant and RO.

The package contains various data items according to the individual package type. Data items include:

- Header Object Data item
- Document Data item that is made by wrapping and signing Documents
- Transmission Data such as the Ticket.

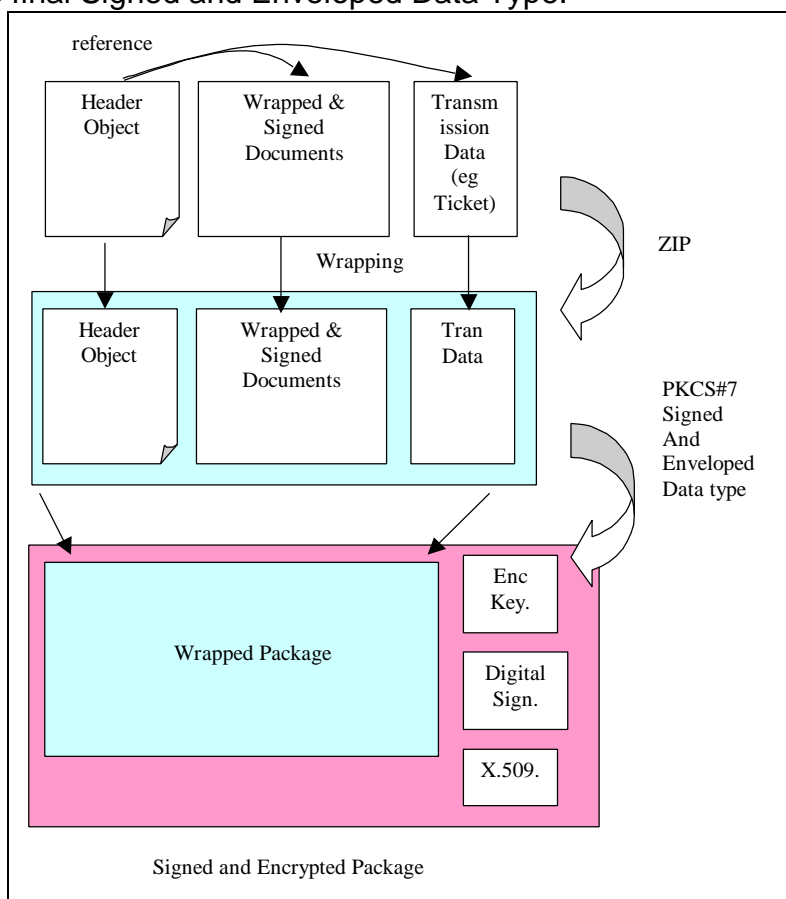
The Header Object Data item indicates the package type, file name of data item, etc. The Header Object Data item is always found in the package. The Header Object Data item is written in XML in accordance with DTD defined in Appendix II.

A package for network transfer is created by making one data block from the multiple data items. The procedure for creating the package is as follows:

- Create a wrapped package by wrapping multiple data items using ZIP
- Create a signed and encrypted package for network transmission by encrypting using the Signed And Enveloped Data Type in PKCS#7

The purpose of the signature is to assure the combination and contents of individual data items, and to ensure that the recipient is able to detect any unauthorized alterations during the transmission. Encryption is to prevent unauthorized interception during data communications.

The Digital Signature for the Wrapper Application Documents may be produced either by the applicant or their representatives. The person that starts the transmission produces the Digital Signature for the final Signed and Enveloped Data Type.



The IP Office then receives the package, opens the data items in the package and decides the role of individual data items in accordance with the documentation in the Header Object Data items.

6 Submission

As shown above, the information exchanged during a transaction is broken into packages. Each phase of the exchange corresponds to the transfer of a package of data sent between the Application and the IP Office.

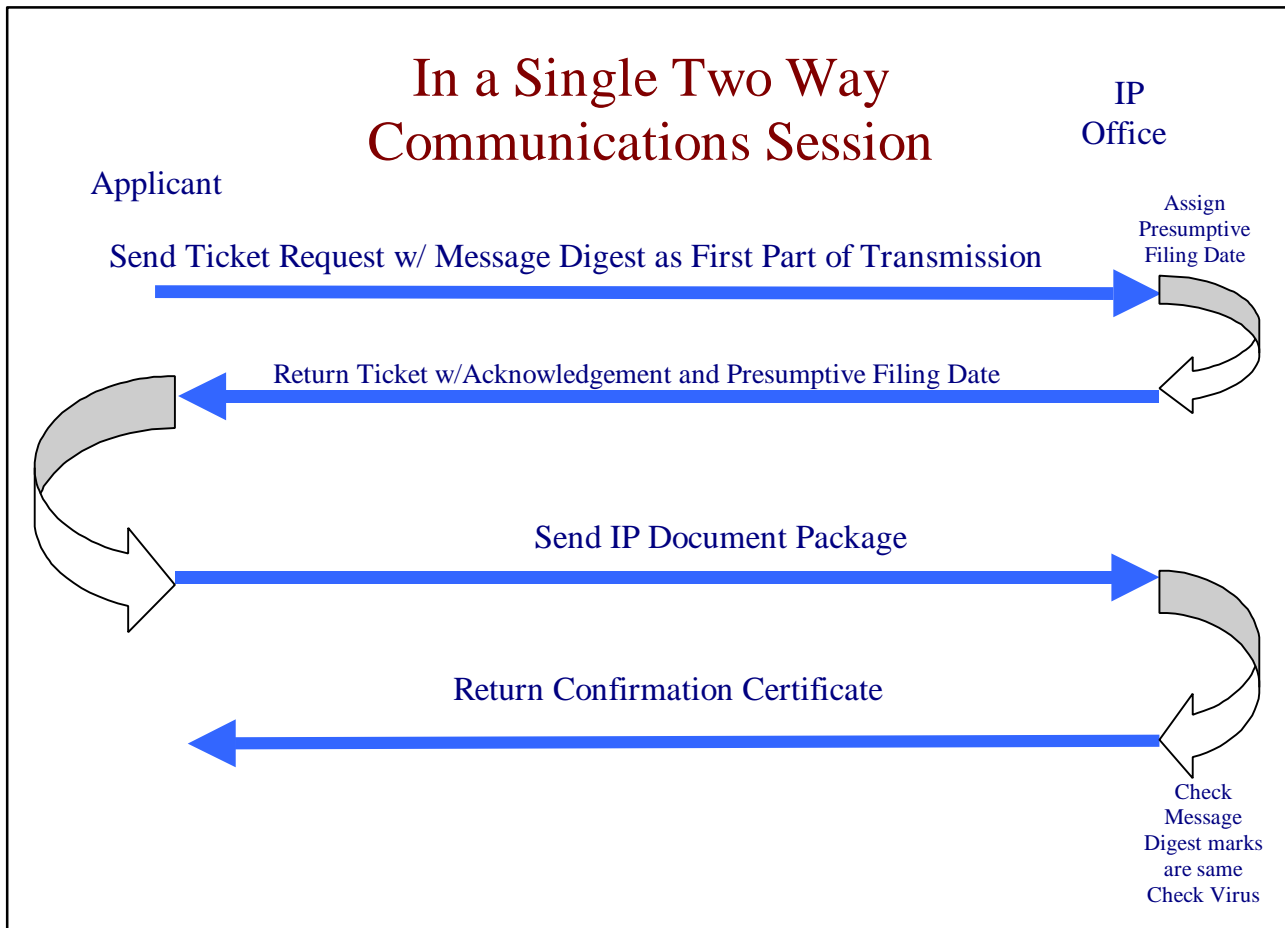
For all transactions, there will be the following four packages :

- Ticket Request

- Ticket
- IP Document Package
- Confirmation Certificate.

For each type of electronic data exchange, the IP Document package will contain the data actually prepared by the applicant (e.g. New Application, Fee Payment, Replacement Claims etc.)

The “**Ticket Mechanism**” operates as follows. :



- An electronic session is established between the applicant and the IP Office.
- Near the beginning of that session, a message digest is transmitted to the Office which is uniquely derived from the wrapped files. The code is such that any change to any of those files will be indicated by a change in that message digest.
- On receipt of that message digest, and as part of the session, the Office sends an acknowledgement to the applicant indicating the date of receipt of the message digest, which will apply to the full documents to come.
- The applicant then continues the session and transmits the complete set of files constituting the IP Document package.
- On receipt of the full set of files, the documents are then checked for the presence of viruses and processed to develop their unique message digest. This is compared to the original message digest that was sent at the beginning of the session. If they match, an acknowledgement of receipt is sent to the applicant. If they do not match, the applicant is informed accordingly. The session can then be ended.

Attachment 4 gives complete details of the communication flow for ticketed communications.

In the event of a communications or message digest comparison problems, the Confirmation Certificate contains information about the problem detected.

6.1 Transfer Protocol

To increase the probability of successful validation, a reliable transport layer protocol shall be used for all transfers between offices. The reliable transport layer protocol serves to assure that all data in transmission has been transferred and re-assembled correctly between the sending and receiving software applications. For this standard, the FTP or the HTTP protocol is used to transfer the package.

The security of communication provided by the encryption within a PKCS#7 Signed And Enveloped Data type will normally be sufficient but, if an IP Office considers it necessary, it may opt for channel level encryption such as SSL or IP Sec to enhance this security.

7 Types of Document Exchange

This Document Exchange Standard includes the following procedures:

National Patent Procedures

- On-line Filing of new patent applications
- [Procedural communications between the Applicant and IP Offices]

PCT Procedures

- On-line Filing of new PCT applications
- [Procedural communications between the Applicant and RO/IB
- Receiving Office to IB (Record Copy)
- RO to ISA (Search Copy)
- IB to ISA
- IB to IPEA]

Non-Patent Procedures

- [Trademark Applications
- Procedural communications between the Applicant and IP Offices]

8 Reference Implementations

As part of the preparation of this standard, the Trilateral offices have prepared two reference implementations (both in JAVA and C++ running on Win NT) that allows other developers to re-use and extend the basic source code provided to build client and procedure specific implementations.

The reference implementations covers the following areas:

- ZIP
- PKCS#7
- Packaging
- Ticket based transfer including return of a Confirmation Certificate.

These are available in source as well as object code.

In addition, standard test data sets are available to verify third-party implementations.

Attachments

Attachment 1. Document Format Requirements

The Trilateral Offices and WIPO are committed to the principle of establishing an open standards environment for electronic exchange of Intellectual Property documents. A notable result of this is: the standard for submitting electronic documents emphasize the use of open standards and will not promote proprietary vendor formats for electronic documents. The reasons for this policy include avoiding the need to maintain the record copies of electronic filings in specific versions of proprietary formats over which the offices have no control.

One desirable feature of commonly used proprietary word processor systems is that they package their electronic documents as a single file such as a .doc or .wps. The proprietary .doc, .wps and other word processor formats combine text, processing instructions, page layout information, raster graphics, vector drawings, tables and other types of data in a single proprietary word processor file.

The Trilateral Offices have selected an open systems alternative to word processor files where electronic documents will be based on using the eXtensible Markup Language (XML) which is being developed to deliver structured data on the World Wide Web. XML documents, like HTML web pages, consist of a character coded text file and zero or more additional files that may be more text or contain binary data such as images and drawings. A typical XML patent application electronic document will consist of a collection of files. An example would be a text file for each procedural document submitted as part of the application plus a text file for the specification of the invention that is accompanied by multiple graphics files (one graphics file for each drawing in the specification). While the XML approach has freed the offices from investing in proprietary word processor formats, the simplicity of the single word processor document file has been lost.

1.1 Images

The facsimile images for use in IP document exchange must meet the following requirements:

- Format
 - TIFF V6.0 with Group 4 compression, Single Strip, Intel Encoded or
 - JPEG
- 200, 300 or 400 dpi
- Max size A4 or Letter size

1.2 PDF

The PDF documents for use in IP document exchange must meet the following requirements:

- Acrobat V3 compatible
- Non-compressed text to facilitate searching
- Un-encrypted text
- No Digital Signatures
- No embedded OLE objects
- All Fonts must either be embedded, Standard PS17 or built from Adobe MM fonts

1.3 XML

All XML documents must conform to one of the DTDs specified in Appendix II.

The character set for all XML documents must be either UTF-8 encoded Unicode UCS-2 (ISO/IEC 10646:193) or ISO-2022-JP encoded JIS-X0208. [For PCT Applications, Chinese GB2312 and Korean KSC 5601 are also acceptable]

Attachment 2. Wrapping Specification (SDIF V2)

The ZIP format published in the PKWARE® PKZIP® Application Note and by Info-ZIP is suitable for use in IP document exchange. Commercial off-the-shelf software libraries and applications for creating ZIP format files are available from several vendors. Use of the ZIP format will provide the benefit of archiving and compression.

2.1 Wrapping of Application Documents

An easy to use, open standards approach is needed to wrap or pack a multi-file electronic document into a single file object for delivery from the applicant to the patent office. Having the applicant create the single file greatly simplifies the handling of the document by the IP Office as it need not track the successful transmission/reception of the individual files. A single file also means that a digital signature can be computed for the application file which can then be used to ensure the data integrity of the entire application.

2.2 Archiving and Compression

The creation of archive files is an approach that has been adopted by the PC, UNIX and Macintosh environments. An archive is a collection of computer files that have been packaged together for backup, to transport to some other location, for saving away from the computer so that more hard disk storage can be made available, or for long term storage. An archive can include a simple list of files or files organized under a directory or catalog structure (depending on how a particular program supports archiving).

Compression is the reduction in size of data in order to save space or transmission time. For data transmission, compression can be performed on just the data content or on the entire transmission unit (including header data) depending on a number of factors.

Content compression can be as simple as removing all extra space characters, inserting a single repeat character to indicate a string of repeated characters, and substituting smaller bit strings for frequently occurring characters. This kind of compression can reduce a text file to 50% of its original size. Compression is performed by a program that uses a formula or algorithm to determine how to compress or decompress data.

The above definitions of archiving and compression include features that are desired for the electronic filing of multi-file patent documents. A suitable archive technique will produce a single file that includes all the component files of an electronic application plus a master directory of the files with information on their type, size, date and time they were last changed and a CRC code for error detection. Data compression of the application content will reduce the amount of time required for online submission and reduce the likelihood of experiencing a transmission error.

2.3 Use of ZIP Files

The ZIP format is a widely used open standard that provides both archiving and compression of data files. The archiving features of ZIP allow the user to collect all the files in a single ZIP directory. All the files in the zip directory along with the directory information are compressed into a single ZIP file object which is suitable for input to a digital signature process. The compression algorithms in the ZIP standard are lossless so the user can be assured that the decompressed result (unZipped) file is identical to the original. The compression techniques used by the ZIP standard achieve the greatest reduction of size (greater than 50%) for text files, but reductions on the order of 10 to 20% for compressed image files are achievable. The error detection features of the ZIP format (which are based on using a 32 bit CRC code) add additional assurance of data integrity.

2.4 ZIP Usage

The files to be zipped shall include all parts of the document identified elsewhere in this specification. All external files referenced by the Specification of the Invention must be included in the ZIP file submission. Filenames included in the central directory of the ZIP file shall comply with the specification for the applicable operating system given elsewhere in this specification.

2.4.1 Directory Structure

All ZIP files must have a flat directory structure. If a collection of files need to be embedded in the ZIP file, then these should be included as a single flat embedded ZIP file.

2.4.2 Compression Algorithms

The ZIP standard allows the compression software to select from among a number of compression algorithms. The default compression method shall be “Deflation” with the normal compression option. This format can be most readily dealt with by UNZIP packages. The “Shrinking” compression method shall not be used because it makes use of a patented Lempel-Ziv-Welch (LZW) compression algorithm protected by a patent held by the UNISYS Corporation.

2.5 PKZIP® Application Note

The ZIP format was originally developed by Phil Katz and incorporated in PKZIP® software for DOS which is available as shareware. PKWARE®, Phil Katz’s company sells commercial versions of ZIP software for many platforms. Phil Katz published the standard for the ZIP format, making it an industry open standard. C programming language source code for the ZIP and UNZIP functions was originally published by a group of independent software developers and appears on the Info-ZIP website <http://www.cdrom.com/pub/infozip/>. Info-ZIP also publishes the ZIP standard on its website. While the ZIP standard is not a formal international standard, the information available on the ZIP format has allowed several third party vendors to develop products that implement ZIP functions on a wide variety of computer platforms. There is good interoperability achieved among the products of these vendors. Most of the third product vendors offer packages that are designed to interoperate with PKWARE® software. A sound strategy is to require applicants to prepare files for submission with any software that claims to be compatible with PKZIP and PKUNZIP. There are currently products available that meet this requirement from WINZip®, DynaZip, NetZip, Info-Zip and others.

The PKZIP® standard can be found as an application note (Revised: 08/01/1998) on the PKWARE® web page <http://www.pkware.com/appnote.html>.

Attachment 3. PKCS#7 Envelope Formats

This document describes the basic specifications of the digital envelope for IP Document Exchange. Following are the preconditions of this specification.

3.1 Scope

In this document, the structure of the digital envelope at the data transfer layer and business data processing layer is defined. The required functions of the digital envelope are given below:

- Giving a digital signature to user data (for authentication or detection of illegal data alteration)
- Encryption of user data

The following matters are NOT described in this Attachment:

- The structure of user data that will be encrypted or to which a digital signature will be given. For example, method of packaging or document format structure etc.
- The method of describing additional information used for data processing at each national patent office. These data elements are not essential information for the applicant and RO.

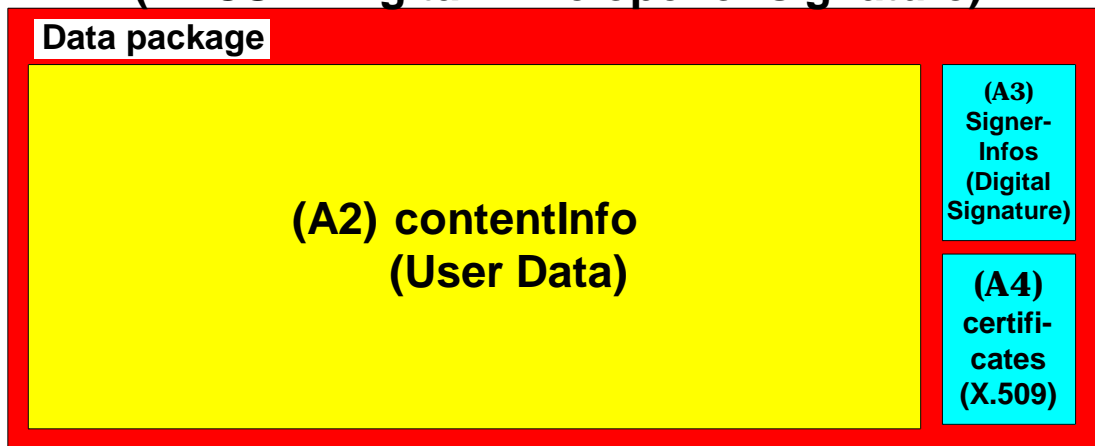
3.2 Definitions

PKCS#7	The PKCS#7 Cryptographic Message Syntax specification, as defined in <i>Internet Draft <draft-hoffman-pkcs-crypt-msg-03.txt> Version 1.5</i>
X.509	X.509 digital certificate standard, as defined in ITU-T Recommendation X.509 (06/97).
Object identifier for sha-1	The object identifier for sha-1 that we adopt is defined in OIW interconnection protocols: Part 12. The definition is below: Sha-1 OBJECT IDENTIFIER ::= {iso (1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26}
Object identifier for RSA encryption	The object identifier for RSA encryption is defined in <i>RSA Encryption Standard PKCS#1</i> . The definition is below: Pkcs-1 OBJECT IDENTIFIER ::= iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1} RsaEncryption OBJECT IDENTIFIER ::= {pkcs-1 1}

Digital envelope for certification

This envelope is used for detecting alterations to user data. The user data, digital signature, and digital certificate of the signer are stored in this envelope.

(A1) Signed Data <Top Level>
(PKCS#7 Digital Envelope for signature)

*Digital envelope for transmission*

This envelope is used for data transmission, to achieve both encryption and alteration detection at the same time. In the case of this envelope, the digital signature is used, not for certification, but for detection of data alteration on the network, so this digital signature does not form part of the business data.

(B1) SignedAndEnvelopedData <Top Level>
(PKCS#7 Digital Envelope for Transmission)



3.3 Common rules for digital envelopes for IP Document Exchange

All digital envelope data should be encoded under DER rules. The DER encoding rule helps the application program to analyze the digital envelope data following only one unique rule.

3.3.1 Digital envelope for the signature

This digital envelope is SignedData type PKCS#7.

Rules for producing the PKCS#7 digital envelope for certification

Table A1 SignedData top level

No.	Item name	PKCS#7 item	Content
1	Version	Version	Set integer value '1'

2	Set of algorithm identifiers	DigestAlgorithms	
2.1	Algorithm identifier	AlgorithmIdentifier	Set ONLY ONE set of algorithm identifiers {sha-1} ¹
3	Content information	ContentInfo	Set one content info (see table A2)
4	Certificates	Certificates	Set one Certificates (see table A4)
5	Certificate revocation lists	Crls	Not used (Set no data)
6	Signer information	SignerInfos	Set one signerInfos (see table A3)

Table A2 contentInfo top level

No.	Item name	PKCS#7 item	Content
1	Content type	ContentType	Set object identifier {pkcs-7 1}
2	Content	Content	Set user data (binary)

Table A3 signerInfos top level

No.	Item name	PKCS#7 item	Content
1	Version	Version	Set integer value '1'
2	Issuer and serial number	IssuerAndSerialNumber	Issuer of certificate and its serial number defined in X.509 spec. (for signer's certificate)
3	Set of digest algorithms	DigestAlgorithm	
3.1	Algorithm identifier	AlgorithmIdentifier	Set ONLY ONE set of algorithm identifiers {sha-1} for making digest of digital signature.
4	Authenticated attributes	AuthenticatedAttributes	Not used (Set no data)
5	Digest encryption algorithm	DigestEncryptionAlgorithm	Set object identifier {pkcs-1 1} (rsaEncryption ²)
6	Encrypted digest	EncryptedDigest	Message digested data; content is encrypted with signer's private key.
7	Unauthenticated attributes	UnauthenticatedAttributes	Not used (Set no data)

Table A4 certificates top level

No.	Item name	PKCS#7 item	Content
1	Set of certificates	ExtendedCertificatesAndCertificates	
1.1	The X.509 certificate	Certificate (defined in X.509 spec.)	Set ONLY ONE set of X.509 certificate data

4.3.2 Details of digital envelope for transmission

¹ sha-1 OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26}

² rsaEncryption OBJECT IDENTIFIER ::= {pkcs-1 1}

This digital envelope is SignedAndEnvelopedData type PKCS#7.

Rules for producing the PKCS#7 digital envelope for transmission

Table B1 SignedAndEnvelopedData top level

No.	Item name	PKCS#7 item	Content
1	Version	Version	Set integer value '1'
2	Recipient information	RecipientInfos	Set ONLY ONE set of recipientInfo (see table B3)
2	Set of algorithm identifiers	DigestAlgorithms	
2.1	Algorithm identifier	AlgorithmIdentifier	Set ONLY ONE set of algorithm identifiers {sha-1}
3	Encrypted Content information	EncryptedContentInfo	Set one encrypted content info (see table B2)
4	Certificates	Certificates	Set one Certificates (see table A4)
5	Certificate revocation lists	Crls	Not used (Set no data)
6	Signer information	SignerInfos	Set one signerInfos (see table A3)

Table B2 EncryptedContentInfo top level

No.	Item name	PKCS#7 item	Content
1	Content type	ContentType	Set object identifier {pkcs-7 1}
2	Content encryption algorithm	ContentEncryptionAlgorithm	Algorithm OBJECT identifier of content encryption. (JPO's tested system: DES in CBC)
3	Encrypted content	EncryptedContent	Encrypted user data

Table B3 recipientInfo top level

No.	Item name	PKCS#7 item	Content
1	Version	Version	Set integer value '1'
2	Issuer and serial number	IssuerAndSerialNumber	Issuer and serial number of certificates that includes the public key for encrypting user data encryption key.
3	Key encryption algorithm	KeyEncryptionAlgorithm	Algorithm OBJECT identifier for encrypting user data encryption key. (JPO's tested system: RSA1024)
4	Encrypted key	EncryptedKey	Encrypted decryption key for user data.

Attachment 4. Ticket Mechanism

This Attachment describes the Data format for each application phase of the Ticket Mechanism.

Ticket is exchanged between the applicant and IP Office with the following protocol.

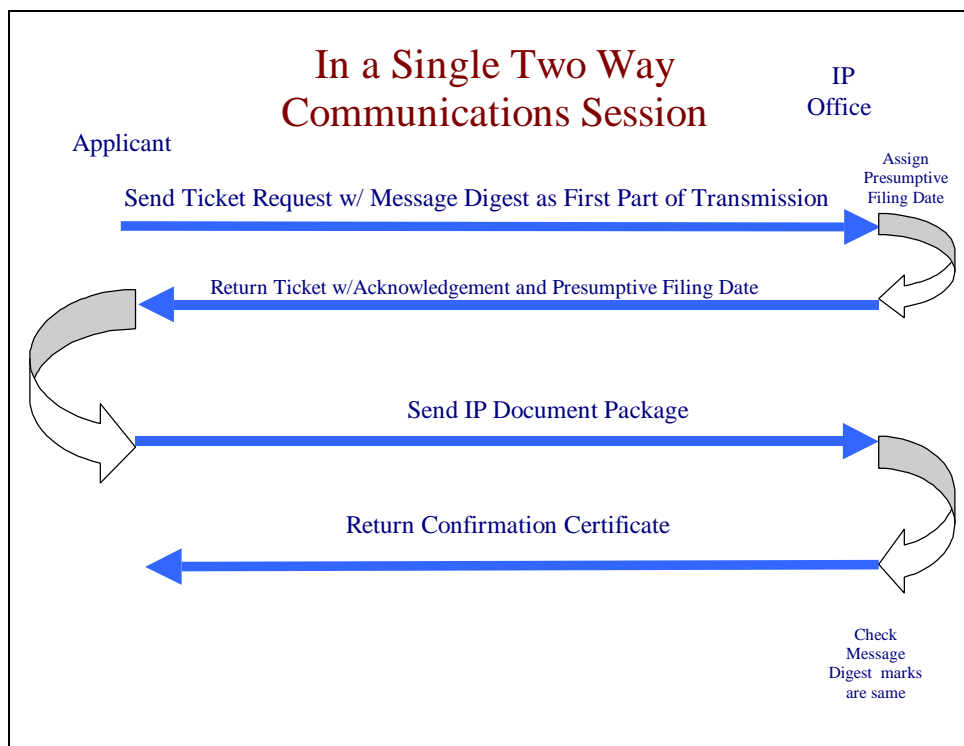


Fig1. Ticket Protocol

Individual protocols in the Ticket system are described below.

4.1 Ticket Request

The Ticket Request is the first packet that is sent to RO. The purpose of sending this packet is to prevent disadvantageous events in recovery measures and transmission speed if the line fails during the submission of an application made with a large Application Documents Data item.

A Ticket Request Data item includes:

- A Message digest created by a Message digest algorithm after wrapping the Documents using ZIP,
- Bibliographic Data and
- A Header Object specifying that the corresponding packet is a Ticket Request.

The Ticket Request is created by wrapping these three Data items with ZIP and packing the resulting ZIP file into a Signed And Enveloped Data type in PKCS#7. This package shall be verified by the client prior to submission. If any errors are detected, this shall be reported to the user and the submission cancelled.

Detailed information on the Header Object Data item is provided in Appendix II. Information on PKCS#7 is provided in Attachment 3.

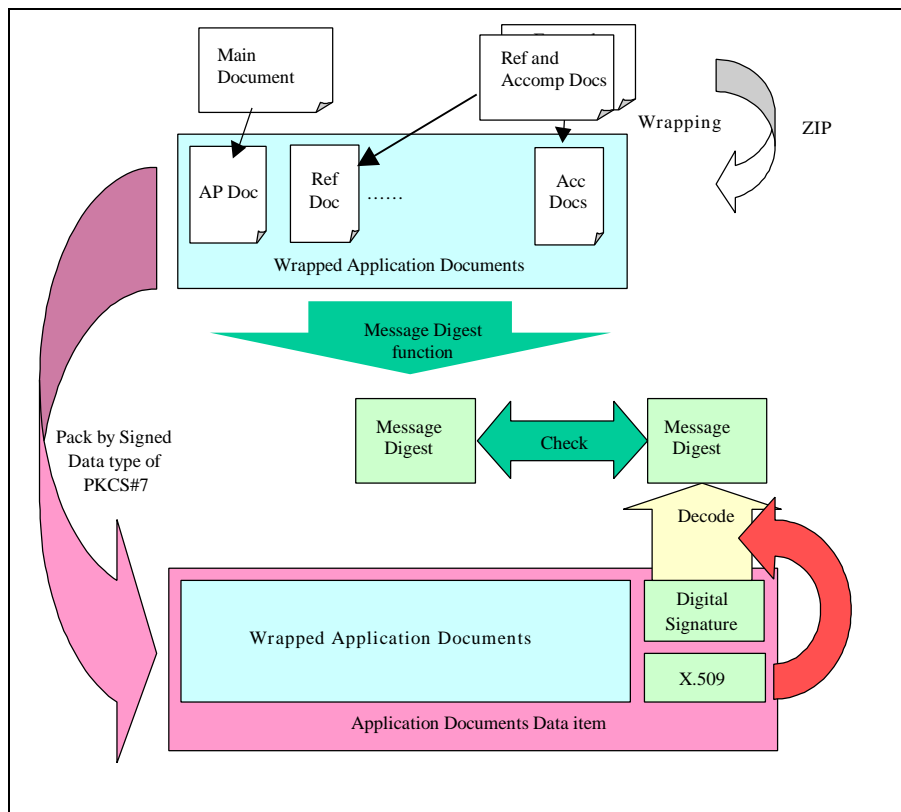


Fig2. Outline of Message digest

Ticket Request

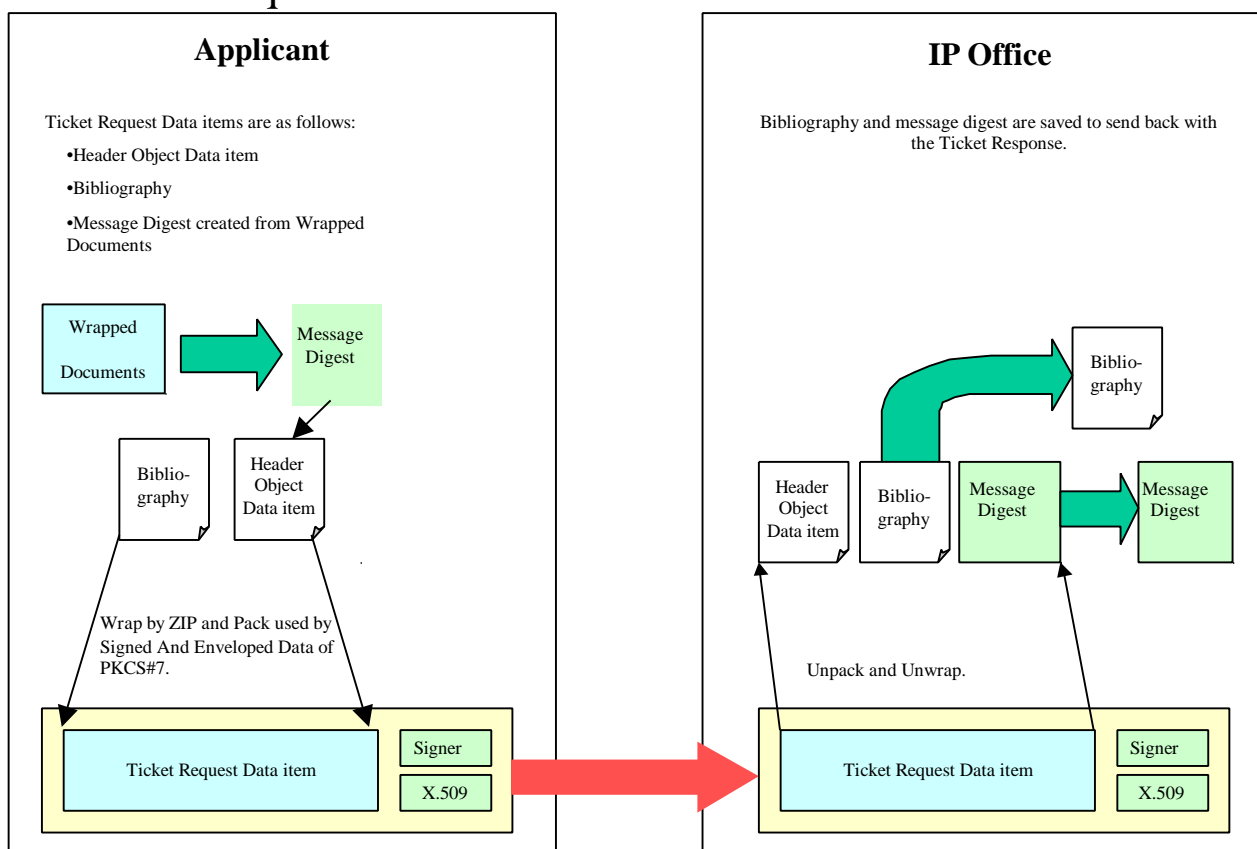


Fig3. Ticket Request

4.2 Ticket Response

The Ticket Response Data item includes a Header Object Data item, a Ticket Data item, and Bibliographic Data.

- The Header Object Data item specifies that the corresponding packet is a Ticket Response.
- The Ticket Data item is created as Signed Data type in PKCS#7 by wrapping the Ticket that includes the Ticket Request Receiving Number, Date Stamp and Expiration Date, and Message digest received from the Ticket Request by ZIP.
- The Bibliographic Data is attached to specify the Ticket Response to the Ticket Request.

The Ticket Response is created by packing with Signed And Enveloped Data type in PKCS#7 after wrapping the Data items by ZIP. New Application can include this Ticket Data item in the Ticket Response.

Detailed information on Header Object Data item is provided in Appendix II. Information on PKCS#7 is available in Attachment 3.

Ticket Response

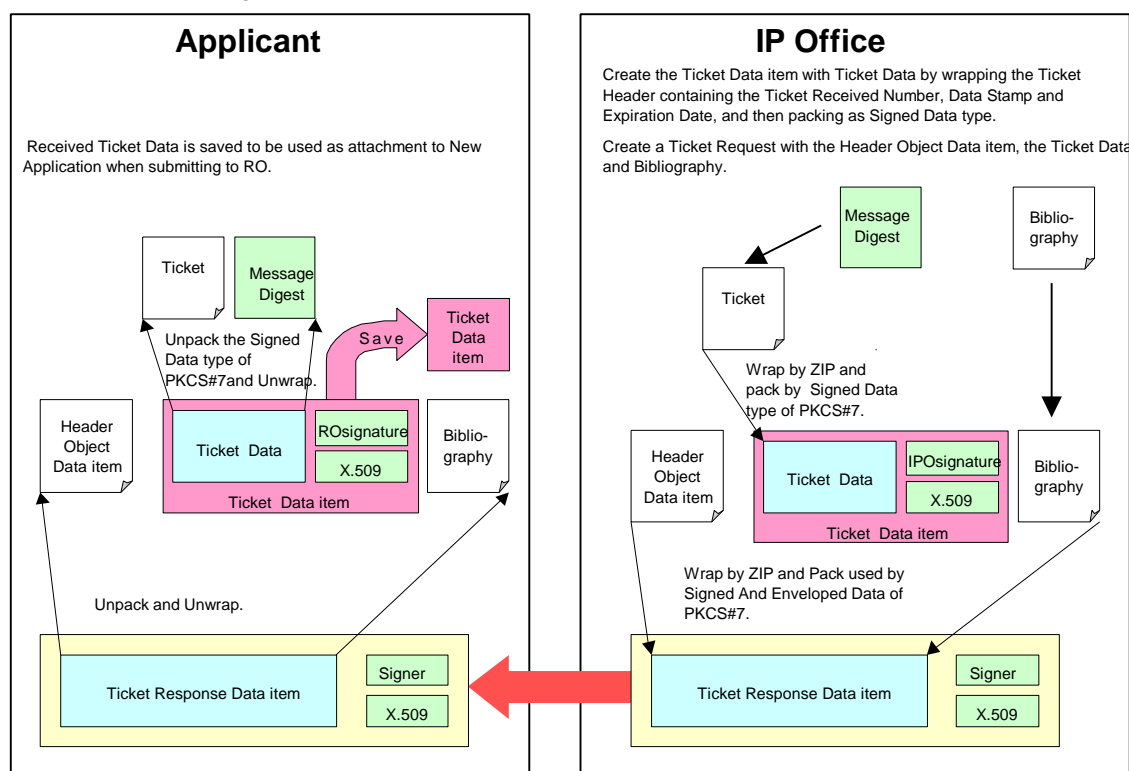


Fig4.Ticket Response

4.3 IP Document

IP Document Data item is created by packing Wrapped Documents using Signed Data Type in PKCS#7. The Wrapped Documents are wrapped in advance using ZIP according to the Wrapping Standard.

IP Document data items include a Header Object Data item specifying what the corresponding packet contains as well as the Ticket Data item received with the Ticket Response.

An IP Document is created as an Envelope by Signed And Enveloped Data type in PKCS#7 after wrapping these data items using ZIP. The Message digest from the unwrapped Ticket Data item is compared with the Message digest of Wrapped Documents included in the IP Document Data item.

Detailed information on the Header Object Data item is provided in Appendix II. Information on PKCS#7 is available in Attachment 3.

IP Document

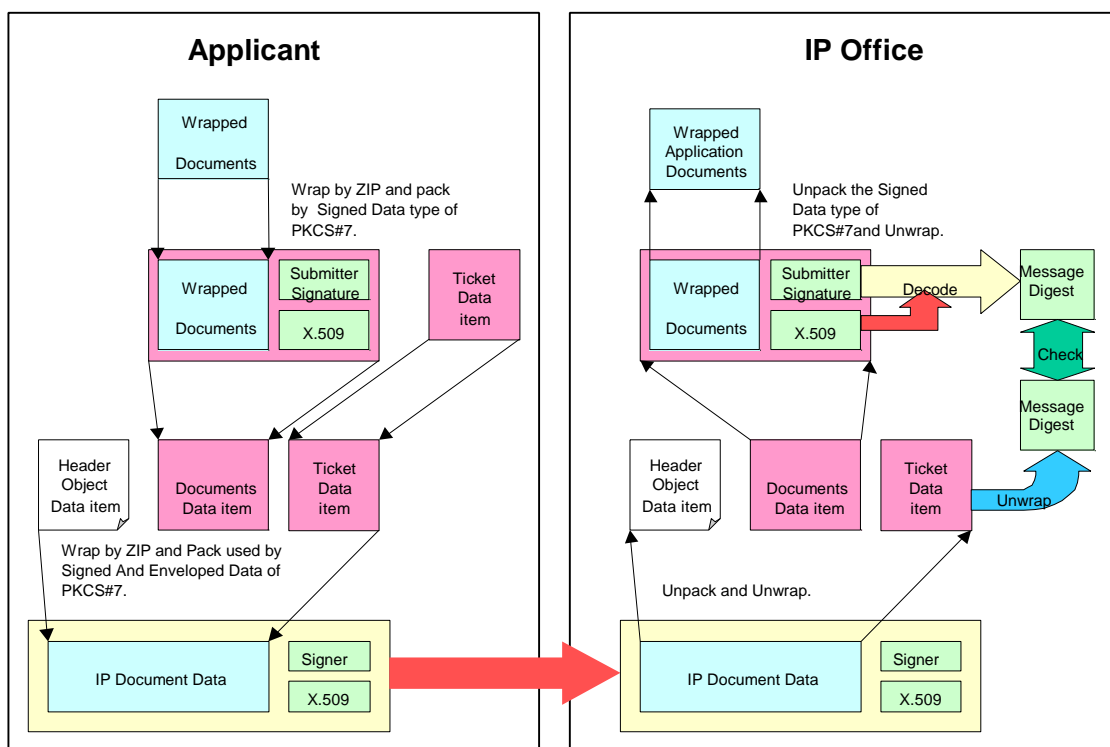


Fig5.New Application

4.4 Confirmation Certificate

The Confirmation Certificate Data item includes a Certificate Data item, a Header Object Data item specifying that the corresponding packet is a Confirmation Certificate, and an Application Documents Data item received with a New Application as an option.

The Confirmation Certificate is created by wrapping and packing the Data item using Signed And Enveloped Data type in PKCS#7.

All application procedures are concluded with a Confirmation Certificate.

Confirmation Certificate

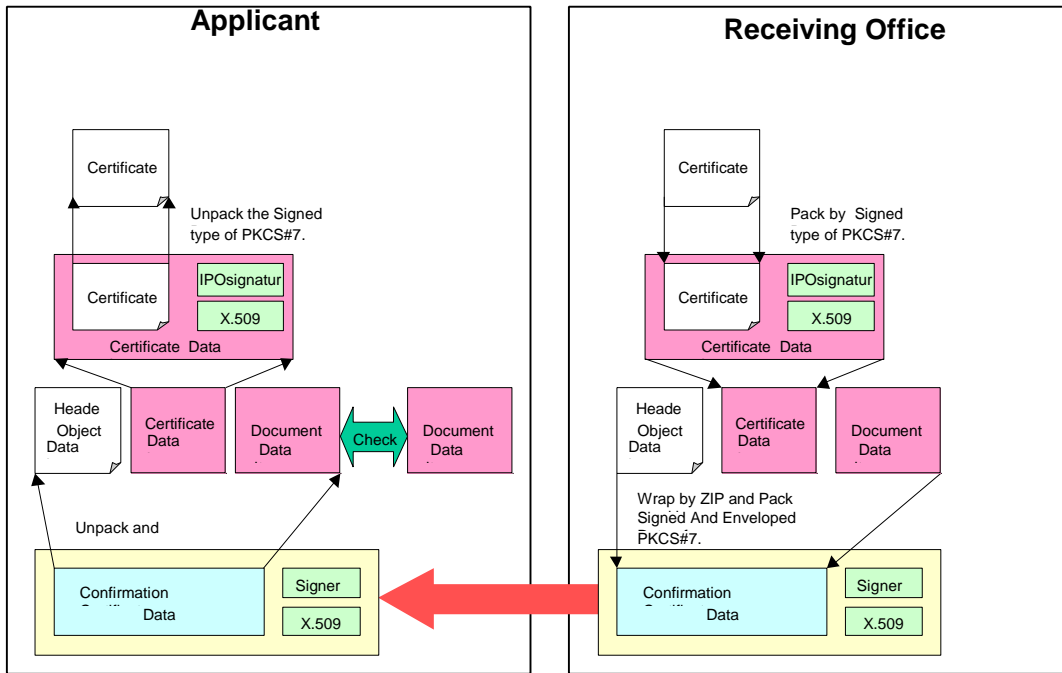


Fig6. Confirmation Certificate

The Confirmation Certificate is used to inform the applicant of the receipt of the application must contain an XML version of this information. It may contain a formatted version of the data in PDF, TIFF and JPEG. These to files are combined in a single ZIP file and signed using the Digital Certificate of the IP Office.

Attachment 5. Records Management Requirements

Long-term desired records management features of automated information systems are listed below. These requirements should be considered for inclusion in developing automated information systems that create, maintain, transfer, or destroy records.

A. Records Creation Requirements

1. Automatically determine the proper disposition of each record created (by record series, if the record is already scheduled), and store the disposition instructions with the record. Allow alteration of the disposition instructions if the schedule changes. Provide a means to manually enter disposition instructions or override those the system selects.
2. Interface transparently with the operating environment and support tools so that certain functions, such as indexing, are transparent to end users.
3. Be compatible with existing paper records.
4. Automatically index all records created in accordance with the IP Office-wide filing scheme (to be developed).
5. Provide automatic electronic date stamp or equivalent on created records.
6. Provide for the creation and storage of “working papers,” both prior to and simultaneous with the addition of indexing and disposition instructions to the record before it can be stored.
7. Convert the storage medium of the record (e.g., hard disk to optical disk).
8. Feature common predetermined retrieval fields (e.g., subject, date, creator office) for ease of mass retrievals.
9. Convert from any format to the accepted standard (e.g., XML, Unicode).
10. Automatically track revisions to a record, document attachments, and addenda (i.e., provide an audit trail).
11. Incorporate margin notes on records without changing the actual record.
12. Integrate different information medium formats (e.g., optical disk, scanned paper, magnetic disk) to make a single record.
13. Link records disposition to the coding/indexing scheme.
14. Create indices based on characteristics such as disposition instructions, key words, subject, or full text.
15. Allow for keyword search capabilities (subject, executive summary, full text, etc.).

B. Records Maintenance Requirements

1. In accordance with either existing records schedules or proposed dispositions, properly manage electronic copies, including the creation and storage of information and reference

- copies. These copies will be handled as records themselves, but will have unique identifiers.
2. Include the capability to protect and distinguish access to classified and otherwise sensitive records.
 3. Integrate the indexing system with the paper indexing system so that retrievals are kept simple (i.e., multiple indexing systems not required).
 4. Maintain an audit trail of record access, changes, etc.
 5. Prohibit changes to a record using the same record identifier (i.e., if a record is changed, a new record should be created and the old record kept intact).
 6. Provide a predetermined number of retrieval fields to simplify retrieval operations.
 7. Recognize and utilize access restrictions such as clearance, need-to-know, etc.
 8. Eliminate the possible loss of records due to system failures or operator errors through automated back-up procedures.
 9. Store records in their native format (e.g., Word for Windows) or in an agreed standard.
 10. Allow for both ease of retrieval and proper physical and electronic safeguarding of records.
 11. Identify vital records (required to restart business after a disaster) Both internally and to the appropriate IP Office manager. These records will require duplicate storage.
 12. Allow screening by the program office official and the records management team.
 13. Automatically display records for screening based on their disposition instructions. This capability will also incorporate features to handle event-driven disposition.
 14. Incorporate features to ease screening for National Laws and Regulations.
 15. Retrieve records based on user level of access. Ensure that the records management team can also retrieve all records created within an agency.
 16. Provide to the user the capability to retrieve by either the index or other predetermined fields. The system will give the user a list of records meeting retrieval criteria.

C. Records Transfer Requirements

1. Generate all required forms to transfer records. The forms and the records should be transferred electronically when possible.
2. Allow for the transformation of records into the proper medium for transfer to archival storage if electronic transfer is not feasible.
3. Verify the quality of records being transferred.
4. Maintain a detailed audit trail of transferred records including date, recipient, losing organization, and descriptions (identifier, file name, etc.).

5. Automatically identify, according to disposition instructions, records requiring transfer. This includes permanent records.

D. Records Destruction Requirements

1. Automatically identify records to be destroyed and notify the owner of the record or the records management team of the destruction requirement. (Destruction date is noted with the disposition authority.)
2. Build in safeguards to avoid accidental destruction of records. This will include a message, which tells the user that the record has not reached its proper disposition period and queries the user to continue with the operation or cancel the operation. The system will have the capability to absolutely delete the record so that it is not retrievable, restorable, or reconstructible. Double checks for deletion/destruction are required.
3. Allow deletion only through the records management function of the system, based on access restrictions.

Attachment 6. Acronyms

PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
SDIF	SGML Document Interface Format
SGML	Standardised Generic Mark-up Language
XML	Extensible Mark-up Language
ePCT	Electronic PCT Application
...	