Public Record Office Victoria
Advice to Victorian Agencies
July 2003, Version 2.0

Advice 12

Advice on
VERS Standard Electronic Record Format
PROS 99/007 (Version 2) Specification 3

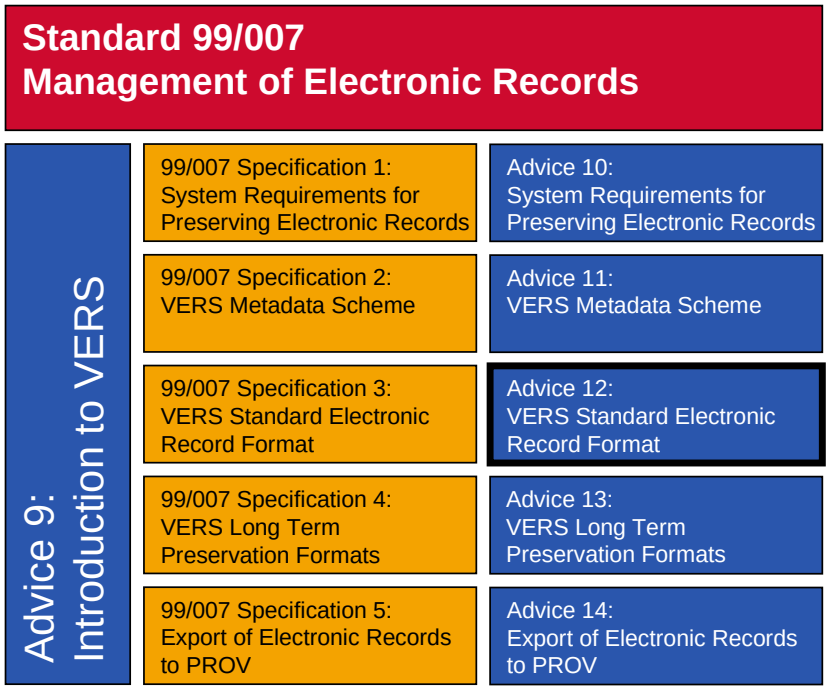
State Government Victoria
Department for Victorian Communities

Further copies of this document can be obtained from the PROV Web site
http://www.prov.vic.gov.au/

Version	Version Date	Details
2.0	31 Jul 03	Released

The Victorian Electronic Records Strategy (VERS)

This document is a guide to *PROS 99/007 Specification 3: VERS Standard Electronic Record Format*. The relationship between the VERS Standard, the Specifications that support this Standard, and the Introduction and Advices that explain VERS is shown below.



These documents have the following purposes:

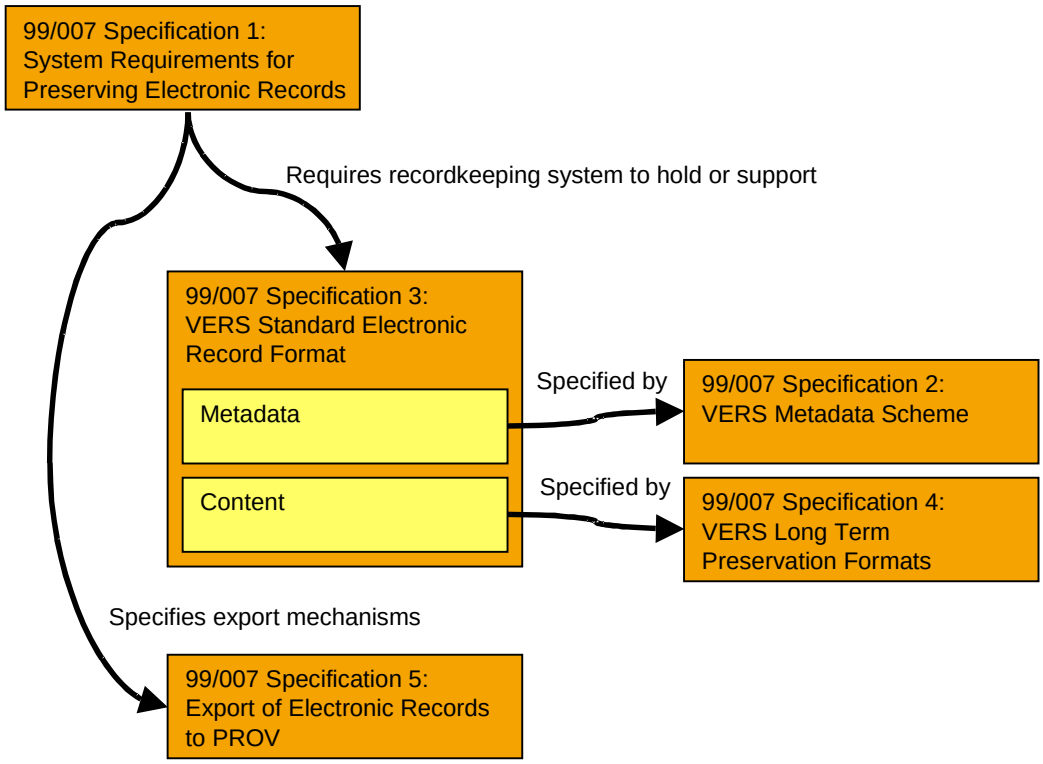
- *Management of Electronic Records*. This document is the Standard itself and is primarily concerned with conformance. The technical requirements of the Standard are contained in five Specifications.
- *Introduction to VERS.* This document provides background information on the goals and the VERS approach to preservation. Nothing in this document imposes any requirements on agencies.
- *Specifications.* These five documents provide the technical requirements that support the Standard. Agencies *must* conform to the mandatory requirements of the specifications, *must* conform to the conditional requirements of the specifications if the appropriate conditions are satisfied, and *may* conform to the optional requirements. Some optional requirements are strongly recommended and these are noted as such.

  The five Specifications are:
  - *Specification 1: System Requirements for Preserving Electronic Records.* This document specifies the overall functions that a recordkeeping system must perform to preserve electronic records for a substantial period.
  - *Specification 2: VERS Metadata Scheme.* This document specifies the metadata that a recordkeeping system must hold to conform to VERS.
  - *Specification 3: VERS Standard Electronic Record Format*. This document contains the technical definition of the VERS Encapsulated Object (VEO) format; the mandatory long-term format for records.

- *Specification 4: VERS Long Term Preservation Formats.* This document lists the data formats that PROV accepts as suitable for representing documents for a significant period.
- *Specification 5: Export of Electronic Records to PROV.* This document lists the approved media and mechanisms by which PROV will accept an export of electronic records.

- *Advices.* These six documents provide background information, explanatory material, and examples in support of the Standard and associated Specifications. None of the information in the Advices imposes any requirement on agencies.

Relationship between Specifications. A second view of the relationship between the five Specifications is shown in the following diagram:



Specification 1 (System Requirements for Preserving Electronic Records) details the overall requirements on a recordkeeping system for preserving electronic records over a significant period. Amongst other requirements, the recordkeeping system must be capable of exporting the records in a standardised format.

The overall features of this standardised format are defined in *Specification 3 (VERS Standard Electronic Record Format)*, but some details are defined in two other Specifications. *Specification 2 (VERS Metadata Scheme)* defines the meaning and allowed values of the metadata that appears in a record. *Specification 4 (VERS Long Term Preservation Formats)* defines the formats in which the record content must be expressed.

Specification 5 (Export of Electronic Records to PROV) defines the mechanisms by which records are exported to PROV.

Relation to Version 1 of this Standard. This version of the VERS Standard completely replaces Version 1 of the Standard. Version 2 is identical in its base requirements, but makes those requirements clearer and more explicit. It also contains a number of conditional and optional extensions to Version 1.

Table of Contents

1 Introduction

Information in this guide is purely informative. Nothing in this guide imposes any requirements on a VERS compliant implementation; requirements are only imposed by the associated Specifications.

The purpose of this guide is to explain the VERS standard electronic record format defined in *PROS 99/007 Specification 3: VERS Standard Electronic Record Format*. The VERS standard electronic record format is also known as a VERS Encapsulated Object or VEO.

As discussed in the Introduction to the Victorian Electronic Record Strategy (Advice 9), a VEO is used to represent a record or folder (file) independently of a recordkeeping system. VEOs may be used as a mechanism to transfer records and folders between two recordkeeping systems, or it may be used as a native format within a recordkeeping system.

2 Goals behind the VEO design

We believe that there are four basic principles that need to be adopted in preserving electronic records. These are:

- *Self-sufficiency*. As far as possible, the electronic record should be independent of systems, outside data, and documentation.
- *Structured textual encoding*. The information that encapsulates the content should be encoded as a structured piece of text rather than as binary data.
- *Integrity*. It must be possible to demonstrate that the record is either unmodified or that any modifications are documented and are authorised.
- *Preservation of authenticity and context*. It must be possible to show who created the record, when it was created, what the record documents, and how the record relates to other records.

2.1 Self-sufficiency

To minimise the possibility of losing a record it is necessary to minimise the dependency of the record on systems, other data, or documentation. The ideal record is *self-sufficient*.

The rationale behind this principle is simple. Increased dependency increases the points of possible failure. If access to a record is dependent on a system, for example, then the loss of that system means the loss of the record.

The most critical dependency with an electronic record is the dependency on the application that interprets a digital object and renders the contents. If the application is lost, typically because it will no longer run on existing computer systems, the records can no longer be displayed and consequently are lost.

For this reason VERS requires content to be migrated to a standard long-term preservation format. Ultimately, the worst-case scenario is that it becomes necessary in the future to implement new software to render record content. In this scenario, the VEO must contain

enough information to allow the format of the content to be identified and sufficient details of the format obtained to allow re-implementation.

No record can be completely self-sufficient because that would require the storage of all the supporting documentation for the long-term preservation format with the record itself. However, if a specification or standard is sufficiently widely published that a copy can reasonably be expected to be found in a public library (or the electronic equivalent) for the foreseeable future, it is sufficient to reference the specification or standard in the record. This issue is discussed further in the advice on *PROS 99/007 Specification 4: VERS Long Term Preservation Formats* (Advice 13).

Electronic records may have other dependencies which may be less obvious. For example, a 'large' collection of records requires some means to allow users to find the records they are interested in. One method is to provide an index. But what happens if this index is lost? The records may still exist, but if it is not possible to recreate the index the contents may be inaccessible. Self-sufficiency requires that a record include a copy of its indexing information. If the external index is destroyed it should be able to be rebuilt using the information stored in the records themselves.

In summary, a good design for an archivable record is record-centric. It minimises the dependency of the record on systems, outside data, and documentation. However, very well-known information can be included by reference to reduce overhead.

2.2 Structured textual encoding

Long-term preservation of information can be viewed as a transmission protocol. The sending computer is the system that creates and (perhaps) initially stores the information. The receiving computer is the future system – as yet unbuilt – that will display the record. A transmission protocol cannot work unless both the sending and receiving hosts precisely agree on the encoding of the information that passes between them. This can be difficult enough to achieve when the two systems can be tested against each other, but in the case of the archiving of electronic information the 'receiving' system has not yet been constructed when the record is 'transmitted' by the 'sending' system.

Thus a well-designed long-term record format has three highly desirable characteristics:

- *Simple encoding*. The encoding of the record should be as simple and as easy to understand as possible.
- *Self-describing*. The smallest units of information in the record should be clearly identifiable, and labelled to indicate their meaning. Consider examining a record and finding a stream of undifferentiated bits. It is impossible to determine where each atom of information starts and stops, the data type of the information, or the meaning of the information. The simplest self-describing encoding is to encode the information as text, with each unit of information delimited by special characters, tag it with a label, and structure the information to show relationships.
- *Self-documenting*. Some units of information will require complex explanations to explain the meaning of the information. Consider a digital signature. It is easy enough to tag the data that forms the signature with the label 'Digital Signature', but to check the signature requires a lot more information. What algorithm was used to generate the digital signature (and what were the values of any parameters)? Exactly what data in the record is covered by the digital signature? Is the digital signature encoded (e.g. has the binary digital signature been turned into text)? An archived record must include sufficient documentation to allow a future user to understand what was done to the

record. A reference to an external publication is sufficient documentation if the external publication will be available indefinitely.

The requirement for a simple, self-describing, and self-documenting encoding suggests a textual encoding. However, there are two problems with the pure textual encoding of a record.

The first problem is efficiency. For example, binary encoding of a 24 bit RGB image requires 3 octets for each pixel. A simple textual encoding would require a minimum of 6 octets (e.g. “0,0,0;”) and a maximum of 12 octets (e.g. “255,255,255;”), or between 200% and 400% space overhead for the RGB data. In addition to the space overhead, both parsing and generating the textual encoding is normally more expensive than parsing and generating the equivalent binary encoding. It is often preferable to use binary encoding for simple efficiency.

The second problem is complexity. Many types of data are inherently complex. Describing a printed page, for example, requires describing the position of every character on the page together with the characteristics of the character such as weight, orientation, and skew. It would be possible to develop a textual encoding to describe a page, but this requires specialist knowledge to ensure that the textual encoding is suitable. It is far preferable to use existing standards for complex data, even if they use complex binary encoding.

It is possible to include binary encodings within an archived object. The key is to:

- Choose a binary encoding that has been published and is therefore available to be referenced, or is sufficiently simple that it can be documented within the record.
- Include documentation on what binary encoding has been chosen in the archived object.

In summary, a good design for a long-term electronic record format will be based on a simple textual encoding that ‘marks up’ the data to indicate its extent, syntactic meaning, semantic meaning, and relationship to other data in the record. The use of binary encodings for specific elements in the record is acceptable when this allows the use of specialist standards, provided the use of these standards is well documented within the record.

2.3 Integrity

In many applications, the archived information is useless, or loses value, unless it can be demonstrated that there have been no unauthorised modifications to the record since it was created.

Two common techniques used to demonstrate integrity are the use of digital signatures and protecting the record using a vault which logs accesses.

A digital signature is a cryptographic technique used to generate a unique signature that depends on the entity signing the object and the contents of the object. Multiple signatures can be used to protect a record from forgery. For example, a record could be signed separately by the registrar of the record and by the system itself. These two signatures protect the record from forgery by any one party acting alone; the registrar's signature ensures that a forgery cannot be perpetrated by a system administrator or by a third party, while the system’s signature ensures that the creator cannot forge the record after the event.

It should be noted that in verifying a digital signature it is necessary to be able to show that the keys used to generate the signature were actually owned by the purported signer at the time that the signature was applied. For this reason it is necessary for the record or the system to hold information about the keys. This point is discussed further in section 5.2.

One of the problems that arises in the use of digital signatures is that the technique will not allow any modifications at all to a record, even authorised modifications. For these reasons, VERS supports the concept of onioning (Version 1) and Modified VEOs (Version 2). These two concepts are equivalent and allow a new, modified version of a record to be created while retaining the original record intact with its digital signatures. These concepts are described more fully in section 3.5.

The more common alternative to protecting integrity by digital signature is to protect integrity by the use of a vault. With this approach, records are protected by the recordkeeping system itself. Records can only be modified using functions provided by the recordkeeping system and all use of these functions is recorded in an audit log. The audit log consequently provides proof that a record retains integrity. In order to do so, it is necessary to show that records may only be modified through the authorised functions and that the audit log itself cannot be modified. Both requirements are difficult to completely fulfil. Both electronic records and audit logs are normally held as files in the computer's file system and these can often be directly manipulated by anyone with sufficient privileges (e.g. a system administrator). This can be controlled by a checksum held by the recordkeeping system, but the question then becomes whether someone with sufficient privileges (e.g. a records manager) can directly manipulate the internal tables to change the checksum.

It is quite possible to show integrity by means of hybrid approaches. For example, one way of complying with VERS is to hold the records in the native form within the recordkeeping system and only express the objects as VERS Encapsulated Objects when they are exported. In this situation the records would be protected using a vault before export and a digital signature afterwards. To demonstrate integrity, the audit log must be extracted and included in the history of the record. In the VERS metadata, the history of the record is documented in M66 Management History and M76 Preservation History (see *PROS 99/007 Specification 2: VERS Metadata Scheme*).

In summary, ensuring integrity can be shown passively by digital signatures, actively by a vault, or by using a combination of both. When it is necessary to be able to modify a record, a digital signature involves complexity and trouble. On the other hand, it can be difficult to absolutely ensure the security of a vault.

2.4 Preservation of authenticity and context

Authenticity and context are documented in the record or folder that contains the record. This documentation is normally represented as metadata. VERS provides extensive metadata to hold this information and this aspect of recordkeeping is discussed in *PROS 99/007 Specification 2: VERS Metadata Scheme*, and its associated advice (Advice 11).

3 VERS long term format (VERS Encapsulated Object)

The VERS long-term format consists of an object (known as a VERS Encapsulated Object or VEO) represented in eXtensible Markup Language (XML). This object contains contextual information about the record or a folder, and may also contain document files, image files, sound files, movie files, etc. The VEO is signed using digital signature technology to ensure integrity.

Formal definitions of all of the metadata described in this section can be found in *PROS 99/007 Specification 2: VERS Metadata Scheme*.

3.1 Generic structure of VEOs

The outermost layers of a VEO are the same for all types of VEOs. This commonality allows management systems to manage VEOs in the same way irrespective of the content of the VEO.

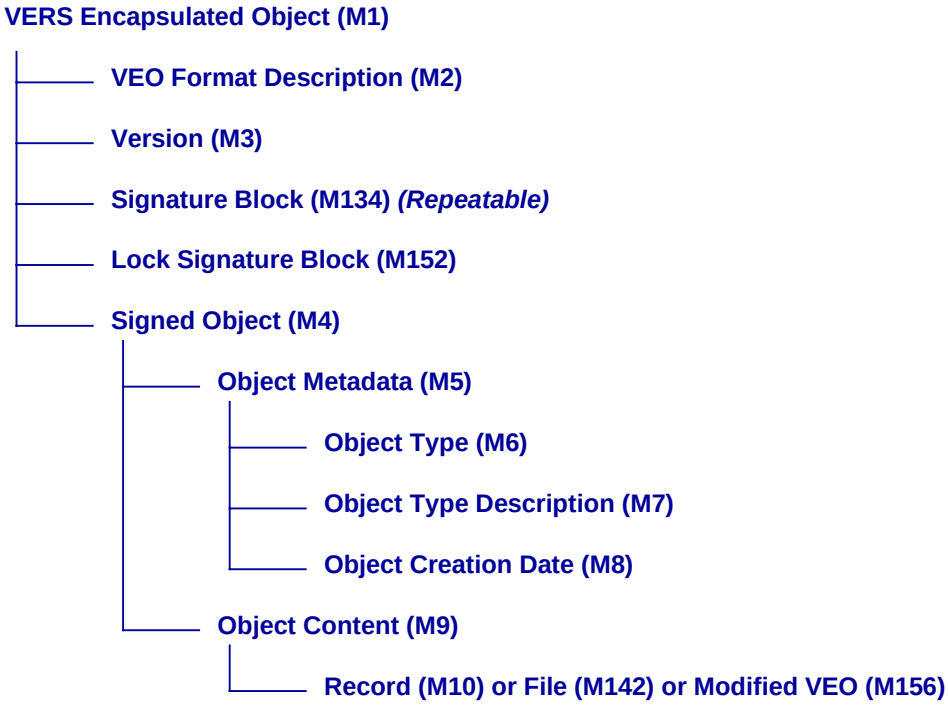


Figure 1. Top level of elements of a VEO.

A VERS Encapsulated Object (VEO) contains VEO Metadata, a Signed Object, one or more Signature Blocks, and a Lock Signature Block.

- *VEO Metadata.* The VEO Metadata consists of the VEO Format Description (M2) and Version (M3) elements.

  VEO Metadata is intended to introduce the VEO to a user who is reading the raw text of the VEO with no knowledge of VEOs or any VERS documentation. The scenario envisaged is that a programmer has been given a VEO, but no supporting documentation, and instructed to extract the record from it. The VEO Metadata occurs right at the beginning of the VEO and states the version, format and encoding of the object and identifies the documents where more information about can be found.

  The VEO Format Description (M2) is a text description of the format and encoding of the VEO, and the Version (M3) is the version of the PROS 99/007 Standard used. It should be noted that no trust can be placed in the information in either of these two elements as they are not protected by digital signature.

- *Signature Block.* A Signature Block element contains the information necessary to verify that the Signed Object has not been tampered with. This information includes a digital signature, the necessary certificates to validate the digital signature, and the identity of the algorithms used to calculate the digital signature. The signed object may

be signed multiple times and so multiple Signature Blocks may be present, one for each digital signature. See section 5.3 for more information about this element.

- *Lock Signature Block.* The Lock Signature Block is used to prevent a forger from 'undoing' modifications. Its use is described in the section on Modified VEOs (see section 3.5.3). This element was added in Version 2 and so will not be present in Version 1 VEOs. A Lock Signature Block must be present in all Version 2 VEOs. (The Lock Signature Block element is marked as optional in the Document Type Definition (DTD), but this is only to allow Version 1 VEOs to validate against the DTD.)
- *Signed Object.* The Signed Object element contains the actual contents of the VEO and will differ depending on the type of VEO. The contents of a Signed Object element are protected from modification by the digital signatures contained in the Signature Block (M134) element.

  Three types of VEOs are currently defined: Record VEOs (see section 3.3), File VEOs (see section 3.2) and Modified VEOs (see section 3.5). Other types of VEOs may be defined in the future.

  A Signed Object element (M4) contains Object Metadata (M5), which describes the object, and the Object Content (M9) element, which contains the content of the VEO. The Object Metadata consists of:
  - Object Type (M6), which indicates the type of the VEO
  - Object Type Description (M7), which is a short textual description of the purpose of the VEO
  - Object Creation Date (M8), which is the date the VEO was created.

  The Signed Object element in a Version 2 VEO must contain a vers:VEOVersion attribute. This attribute duplicates the information in the Version (M3) element. The reason for this duplication is that the Version (M3) element is not protected by the digital signature and can therefore be changed at will. The vers:VEOVersion attribute, however, is covered by the digital signature and so cannot be modified without detection.

An example of the basic structure expressed in XML follows.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<!DOCTYPE vers:VERSEncapsulatedObject SYSTEM "vers.dtd">
<vers:VERSEncapsulatedObject
  xmlns:vers="http://www.prov.vic.gov.au/gservice/standard/pros99007.htm"
  xmlns:naa="http://www.naa.gov.au/recordkeeping/control/rkms/contents.html">
 <vers:VEOFormatDescription>
  <vers:Text>
This record conforms to the structure defined in "Management of Electronic
Records, PROS 99/007 (Version 2.0)" Public Record Office Victoria, 2003.
The structure of this record is represented using Extensible Markup Language
(XML) 1.0, W3C, 1998.
  </vers:Text>
 </vers:VEOFormatDescription>
 <vers:Version>2.0</vers:Version>
 <vers:SignatureBlock vers:id="Revision:1-Signature:1">
 [...]
 </vers:SignatureBlock>
 <vers:LockSignatureBlock vers:signsSignatureBlock="Revision:1-Signature:1">
  [...]
 </vers:LockSignatureBlock>
 <vers:SignedObject vers:VEOVersion="2.0">
  <vers:ObjectMetadata>
   <vers:ObjectType>Record</vers:ObjectType>
   <vers:ObjectTypeDescription>
This object contains a record; that is a collection of information
that must be preserved for a period
   </vers:ObjectTypeDescription>
   <vers:ObjectCreationDate>
    2003-03-20T11:27:40-10:00
   </vers:ObjectCreationDate>
```

```
  </vers:ObjectMetadata>
  <vers:ObjectContent>
   <vers:Record>
    [...]
   </vers:Record>
  </vers:ObjectContent>
 </vers:SignedObject>
</vers:VERSEncapsulatedObject>
```

3.2 File VEOs

File VEOs contain the information associated with a recordkeeping folder (i.e. file).[1]

In the paper world, a folder contains a sequence of related records; therefore in VERS each Record VEO is expected to be associated with a File VEO. File VEOs may contain descriptive information not present in the individual records.

Figure 2. Top level elements of a File VEO.

The contents of a File VEO are:

- *File Metadata.* The File Metadata (M143) element contains metadata describing the folder; this is largely identical to the record level metadata of a Record VEO. The File Metadata is defined in *PROS 99/007 Specification 2: VERS Metadata Scheme*) and a discussion can be found in Advice 11.
- *File Disposal.* The File Disposal (M145) element contains information about the disposal of a folder (and the records it contains) and will only be present if the folder has, in fact, been disposed of. The File Disposal metadata is defined in *PROS 99/007 Specification 2: VERS Metadata Scheme*) and a discussion can be found in Advice 11.

Two examples of File VEOs are given in section 7.

File VEOs are designed to be used for exchanging information between two recordkeeping systems and could not be modified in Version 1. In Version 2, however, the contents of a File VEO may be modified using the Modified VEO (see section 3.5).

It should be noted that File VEOs do not physically contain the Record VEOs contained in the folder. Instead, the Record VEOs are implicitly linked to the File VEO by means of the VEO Identifier (M99) element. Each Record VEO is linked to the folders on which it is filed by means of the File Identifier (M102) element within the VEO Identifier (M99).

[1] 'File' is the traditional recordkeeping term. Since Version 1 of VERS was released, PROV has come to prefer the term 'folder' as this avoids confusion between computer files and recordkeeping files. Unfortunately, the VEO was named before it was recognised that it was necessary to make this distinction.

3.3 Record VEOs

A Record VEO is the most common VEO and contains one electronic record. In VERS, an electronic record consists of one or more Documents, each of which consists of one or more Encodings.

A Document is an independent portion of record. An example of this would be the record of a meeting (below) which consists of two documents: the minutes and a presentation given at the meeting

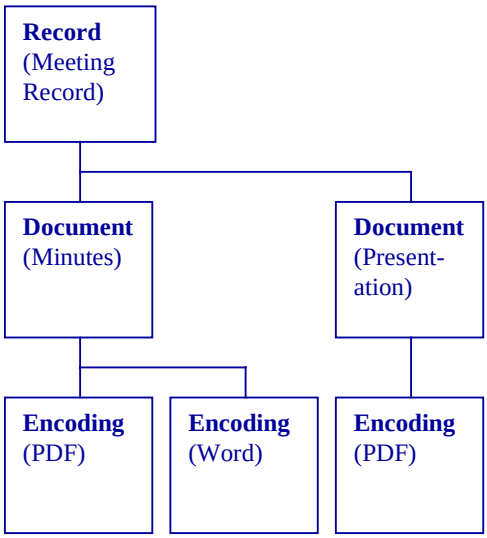


Figure 3. Example of a record that contains multiple Documents and Encodings.

An Encoding is a physical representation of a Document. In the diagram above, the minutes are represented twice: once as a PDF file and once as a Word file. The presentation, however, is only represented by one Encoding (in PDF).

VERS does not require that a recordkeeping system must support multiple Documents within a record (the VERS standard must support all recordkeeping systems, including those which do support multiple Documents in a record). Even if the recordkeeping system does support multiple Documents in a record, the decision as to whether to use this functionality is up to an agency and, potentially, to individual users within the organisation.

Similarly, VERS does not require that a recordkeeping system must support multiple Encodings for each Document. A VERS-compliant recordkeeping system may only allow a Document to have one physical representation.

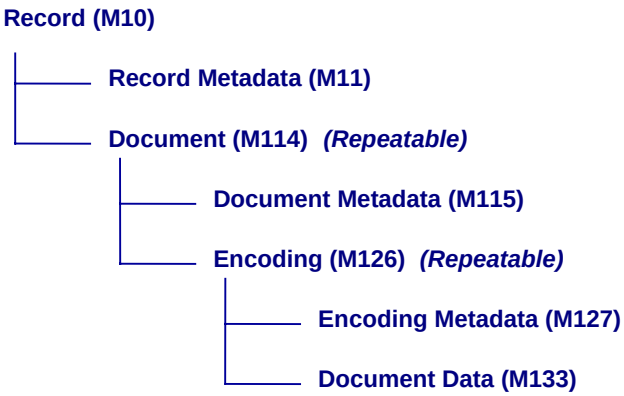


Figure 4. Main structural elements of a Record VEO.

A Record VEO contains all of the information associated with one record. The VEO contains all of the Documents and all of the Encodings associated with one record. The broad structure of a Record VEO is shown in Figure 4. The elements are:

- *Record Metadata.* The Record Metadata (M11) element describes the record as a whole. Primarily, this encompasses what the record is, how it relates to other records, and its history. This metadata is described in *PROS 99/007 Specification 2: VERS Metadata Scheme,* and a discussion on the use of this metadata can be found in Advice 11.
- *Document.* The Document (M114) element contains a single Document within a record and may be repeated. A Document contains:
  - *Document Metadata.* This element (M115) contains metadata that describes the Document, that is, information that distinguishes this Document from other Documents and from the record as a whole. Again, this metadata is described in *PROS 99/007 Specification 2: VERS Metadata Scheme,* and a discussion on the use of this metadata can be found in Advice 11.
  - *Encoding.* This element (M126) contains a representation of the Document, for example a PDF file or a Word file. A Document may have multiple Encodings. An Encoding contains:
    - *Encoding Metadata.* This element (M127) describes the file format. Again, this metadata is described in *PROS 99/007 Specification 2: VERS Metadata Scheme,* and a discussion on the use of this metadata can be found in Advice 11.
    - *Document Data.* This element (M133) contains the actual physical representation of the Document.

The contents and structure of records, Documents and Encodings are largely unchanged from Version 1. However, one change from Version 1 is the ability to structure Documents within a record. This feature is described in the next section.

3.4 Document structure

In Version 2, Documents within a record can be structured. That is, a Document can contain other Documents. This feature is optional and a VERS-compliant system does not have to support it.

An example of the use of structured Documents is the record of an email message.

A received email consists of header information, at least one email body (and possibly several alternate email bodies), and, optionally, one or more attachments. The purpose of this information is as follows:

- The header information contains information about the email. This includes the familiar ‘Subject’, ‘From’ and ‘To’ fields. It also includes more technical information describing which machines handled the email in the transmission from the sender to the receiver.
- The alternate email bodies are intended to represent the same email message using different formatting commands. For example, an email may include a HTML version of the message and a plain text version. The email program should display the HTML version, if it is capable of doing so, otherwise it will display the plain text version.
- The attachments are supplementary information that are not interpreted by the email program itself, but are detached or viewed by applications on the receiving computer.

When an email program presents an email to a user, only part of the information in the email is actually displayed. First, the email program selects and displays *some* of the email headers (typically the 'Subject', 'From', 'To' and 'Cc' fields). Second, it selects *one* of the alternate email bodies and displays it. Finally, the client indicates that attachments are present, but the user usually has to explicitly act to open them.

When capturing a record of an email it is often not sufficient to simply capture the actual email message. This is because the user actually saw very little of the actual email message. The user saw a subset of the headers, one of the alternate bodies, and may not have viewed any of the attachments.

Using structured Documents it is possible to capture a record both of what the user actually saw and what was sent.

A possible record of an email, created using structured Documents, is shown in Figure 5.

The key Document within the record is a facsimile of the email message that was actually presented to the user. In Figure 5 this is represented by the ‘email body’ Document. This would be formatted to reflect how the email body was displayed when the user saw it, including the headers actually displayed and the icons indicating any attachments. The use of this Document clearly differentiates between what the receiver of the email saw when they read the email, and the alternative bodies and additional headers that the user did not see.

Attachments to the email can then be included as sub-Documents beneath the email body Document, clearly differentiating between the body and the attachments (which the user may not have opened). Finally, additional Documents can be used to represent the remaining header information not presented to the user (this information shows how the email was transmitted and may be critical in demonstrating the integrity and authenticity of the email).

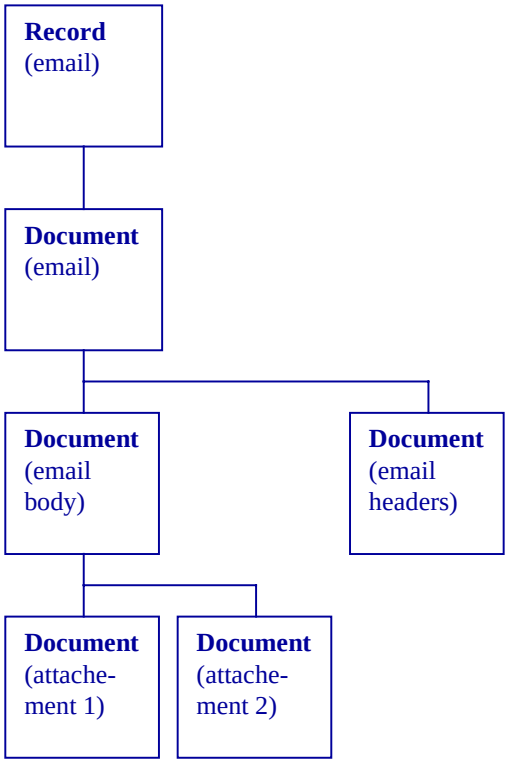


Figure 5. A record containing structured Documents

3.4.1 Method of indicating the structure within records

In VERS, the Documents within a record are indicated by attributes contained in the vers:Document (M114) element. Another implementation option would have been to define a Structured Document element which could contain Documents or other Structured Documents. This approach would have been much cleaner, but would have meant that Version 1 VERS systems would not be capable of recognising Documents in a Version 2 VEO.

The structuring information is represented by three attributes that may be contained within a Document (M114) element.

- The vers:id attribute uniquely identifies this Document within a VEO (including any older versions of the Document in the case of a Modified VEO).
- The parentDocument attribute contains the vers:id attribute of the superior Document. The topmost Document does not contain a parentDocument attribute.
- The subordinateDocuments attribute contains the vers:id attributes of the subordinate document. A leaf Document (at the bottom of the tree) has no subordinateDocuments attribute

Figure 6 shows a diagram of the record in Figure 5 illustrating the use of these three attributes.

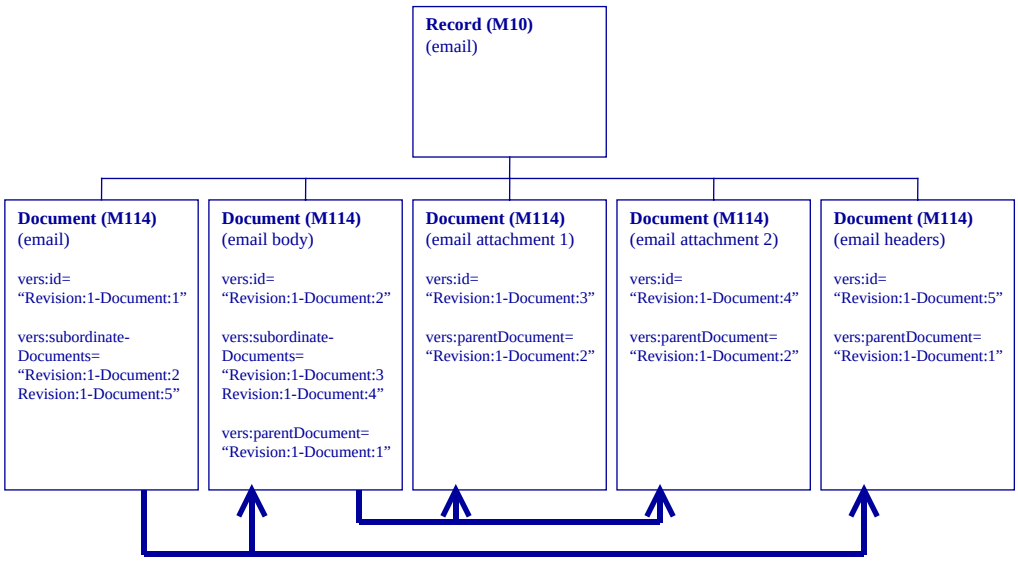


Figure 6. The structured record shown in Figure 5 represented diagrammatically as a VEO.

Expressed as XML, the email record is as follows (note that elements not relevant to this discussion have been omitted):

```
 <vers:SignedObject vers:VEOVersion="2.0">
  <vers:ObjectMetadata>
[...]
  <\vers:ObjectMetadata>
  <vers:ObjectContent>
   <vers:Record>
    <vers:Document
      vers:id="Revision:1-Document:1"
      vers:subordinateDocuments="Revision:1-Document:2 Revision:1-Document:5">
     <vers:DocumentMetadata>
[...]
      <vers:DocumentTitle>
       <vers:Text>Email</vers:Text>
      </vers:DocumentTitle>
     </vers:DocumentMetadata>
[...]
    </vers:Document>
    <vers:Document
      vers:id="Revision:1-Document:2"
      vers:subordinateDocuments="Revision:1-Document:3 Revision:1-Document:4"
      vers:parentDocument="Revision:1-Document:1">
     <vers:DocumentMetadata>
[...]
      <vers:DocumentTitle>
       <vers:Text>Email Body</vers:Text>
      </vers:DocumentTitle>
[...]
     </vers:DocumentMetadata>
     <vers:Encoding vers:id="Revision:1-Document:2-Encoding:1">
      <vers:DocumentData
        vers:id="Revision:1-Document:2-Encoding:1-DocumentData">
JVBERi0xLjMNJeLjz9MNCjkwIDAgb2JqDTw8IA0vTGluZWFyaXplZCAxIA0vTyA5MiANL0
[...]
JUVPRg0=
      </vers:DocumentData>
     </vers:Encoding>
    </vers:Document>
    <vers:Document
      vers:id="Revision:1-Document:3"
      vers:parentDocument="Revision:1-Document:2">
     <vers:DocumentMetadata>
```

```
[...]
      <vers:DocumentTitle>
       <vers:Text> Email Attachment 1 </vers:Text>
      </vers:DocumentTitle>
[...]
     </vers:DocumentMetadata>
     <vers:Encoding vers:id="Revision:1-Document:3-Encoding:1">
[...]
      <vers:DocumentData
        vers:id="Revision:1-Document:3-Encoding:1-DocumentData">
JVBERi0xLjMNJeLjz9MNCjkwIDAgb2JqDTw8IA0vTGluZWFyaXplZCAxIA0vTyA5MiANL0
[...]
JUVPRg0=
      </vers:DocumentData>
     </vers:Encoding>
    </vers:Document>
    <vers:Document
      vers:id="Revision:1-Document:4"
      vers:parentDocument="Revision:1-Document:2">
     <vers:DocumentMetadata>
[...]
      <vers:DocumentTitle>
       <vers:Text> Email Attachment 2 </vers:Text>
      </vers:DocumentTitle>
[...]
     </vers:DocumentMetadata>
     <vers:Encoding vers:id="Revision:1-Document:4-Encoding:1">
[...]
      <vers:DocumentData
        vers:id="Revision:1-Document:4-Encoding:1-DocumentData">
JVBERi0xLjMNJeLjz9MNCjkwIDAgb2JqDTw8IA0vTGluZWFyaXplZCAxIA0vTyA5MiANL0
[...]
JUVPRg0=
      </vers:DocumentData>
     </vers:Encoding>
    </vers:Document>
    <vers:Document
      vers:id="Revision:1-Document:5"
      vers:parentDocument="Revision:1-Document:1">
     <vers:DocumentMetadata>
[...]
      <vers:DocumentTitle>
       <vers:Text> Email Headers </vers:Text>
      </vers:DocumentTitle>
[...]
     </vers:DocumentMetadata>
     <vers:Encoding vers:id="Revision:1-Document:5-Encoding:1">
[...]
      <vers:DocumentData
        vers:id="Revision:1-Document:5-Encoding:1-DocumentData">
JVBERi0xLjMNJeLjz9MNCjkwIDAgb2JqDTw8IA0vTGluZWFyaXplZCAxIA0vTyA5MiANL0
[...]
JUVPRg0=
      </vers:DocumentData>
     </vers:Encoding>
    </vers:Document>
   </vers:Record>
  </vers:ObjectContent>
 </vers:SignedObject>
```

3.4.2 Organising Documents within records

When organising Documents to appear in a VERS record, the first document must be the topmost Document. The remaining Documents may be in any order, but it is recommended that the Documents are ordered via a depth-first traversal of the document tree. A depth-first traversal is one where the descendants of a Document appear before its siblings appear. The depth-first traversal of the email example (Figure 5) is shown in Figure 7.

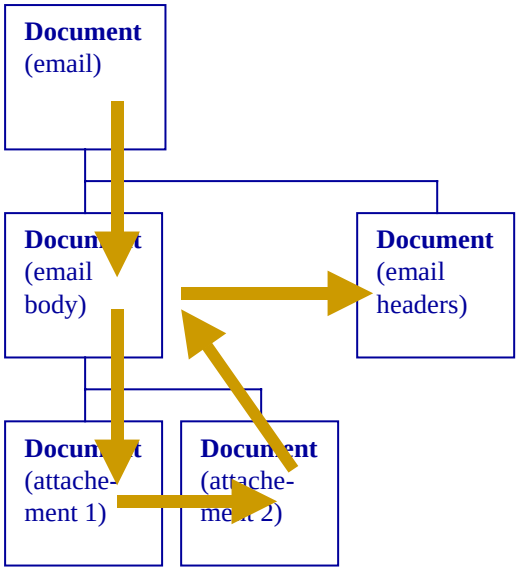


Figure 7. The depth-first traversal of the Documents shown in Figure 5. Note that the descendants of the email body (the two attachments) are visited before its sibling (the email headers) is visited.

VERS systems that do not implement document structuring (i.e. Version 1 systems and Version 2 systems that do not implement document structuring) will present the documents in the order that they appear in the VEO.

3.4.3 Non-leaf documents need not contain encodings

A non leaf Document need not contain any Encodings, in this case the Document merely provides structure to the Record. A non-leaf Document is any Document that has subordinate Documents (i.e. contains a vers:subordinateDocuments attribute).

In the email example the email and email body Documents are non-leaf Documents. The email (topmost Document) exists simply to provide part of the structure and does not contain any content. If the example XML given in section 3.4.1 is examined, the reader will note that Document 1 (the topmost document) does not contain an Encoding element.

3.4.4 Additional structural attributes

In addition to the three structuring attributes (vers:id, vers:subordinateDocuments and vers:ParentDocument), the Document (M114) element can contain two other attributes (these are not shown in Figure 6):

- *vers:subordinateDocumentRelationship.* This indicates how the subordinate Documents are related to each other. Usually, the subordinate Documents form a sequence and should be presented one after the other from the first to the last. However, they may be a set (in which case they may be presented in any order), or alternatives (in which case one should be selected and the remaining Documents not presented at all).
- *vers:presentThisDocument*. This is a boolean flag. This is usually set to true, in which case the Document will be displayed. If false, the Document need not be displayed to a user of the records, the assumption being that this Document simply aids structuring of the Documents in the record. An example is the root Document in the email; this is simply a container for the two sub-Documents and provides no useful information. Accordingly, this could be marked as presentThisDocument=”false”.

3.5 Modifying records and Modified VEOs

When a recordkeeping system holds folders and records internally in the VEO format the digital signatures prevent the contents of those folders and records from being modified. Accordingly, in both Version 1 and Version 2 of the Standard there is a mechanism that allows a new, modified version of a record to be created which contains the original record complete with digital signatures. In Version 1 this mechanism was known as an 'Onion' record, and only allowed a Record VEO to be modified. In Version 2 a new mechanism has been defined (known as a 'Modified VEO') that allows for the modification of both records and folders.

Recordkeeping systems that only produce VEOs upon export need not implement either mechanism. Version 2 systems must only generate Modified VEOs and must not use the onioning mechanism. Version 2 systems that can import VEOs must be able to handle Version 1 VEOs, including those that have been produced using the onion mechanism.

3.5.1 ‘Onion’ records

Version 1 allowed Record VEOs to be modified by onioning. This approach is shown in Figure 8. To modify a Record VEO, a new Record VEO (the ‘Onion VEO’) is created. The new Record VEO contains the complete original VEO, including the original digital signatures, as a Document. The new Record VEO also contains the modified record metadata. Since the new Record VEO contains the unaltered original VEO, complete with digital signature, the integrity of the original VEO can still be verified. The digital signatures on the new Record VEO cover both the new modified Record Metadata and the original VEO, and so the integrity of the modified metadata and the relation with the original VEO is protected. If necessary, this process can be repeated by wrapping the modified Record VEO within a new VEO, hence the 'onion' analogy.

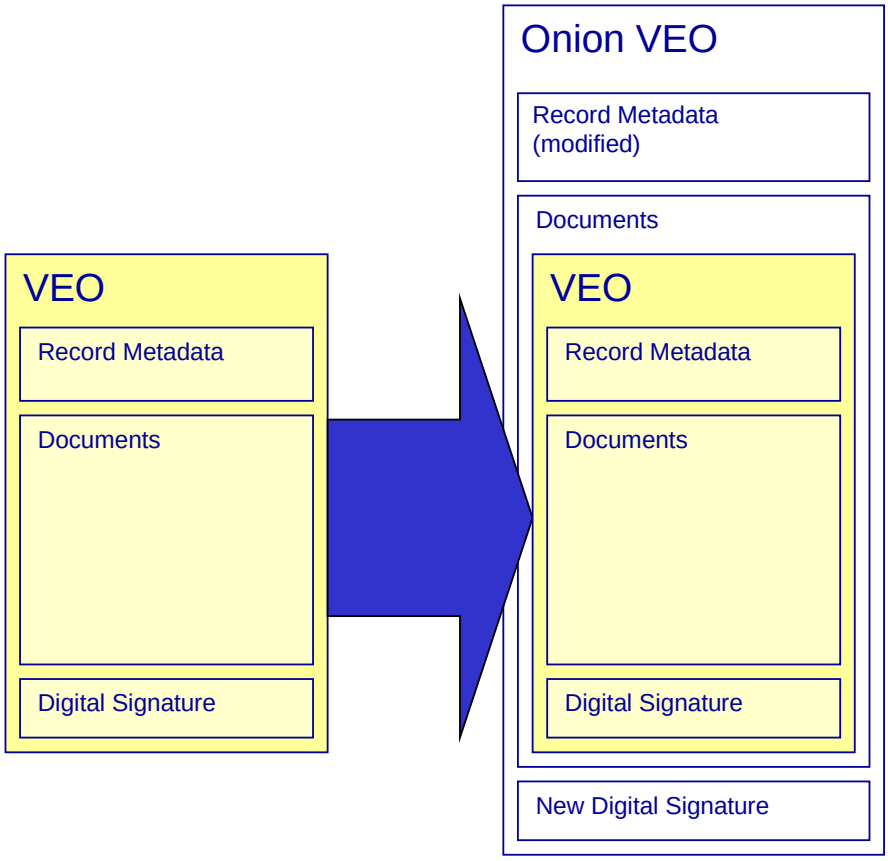


Figure 8. Creation of an onion record. The original VEO is included complete within the new VEO as a Document.

The process of onioning has three problems:

- It is not possible to modify any of the Documents within a record. In particular it is not possible to:
  - Add additional Documents. This may need to occur if the user omits a relevant Document from the record.
  - Delete Documents. This may need to occur if a Document has been incorrectly incorporated in the record.
  - Modify the metadata associated with a Document or Encoding. This may need to occur if a Document or Encoding has been incorrectly described.
  - Add an Encoding to a Document. This may occur if a long-term preservation format is replaced by a new preservation format and all instances of the old format are migrated.
  - Delete an Encoding from a Document. This may occur when a particular format can no longer be processed.
- It is possible to discard modifications. Consider the onion VEO in Figure 8. It is possible to extract the original VEO from the onion record, and this extracted VEO will be a perfectly valid VEO. If it was then possible to replace the onion VEO in the recordkeeping system with the original VEO, the modifications would have been effectively discarded with no way of determining that this discarding occurred. As there may be more than one layer of modifications, it is clear that any number of layers of the onion can be discarded.
- It is not possible to modify a File VEO as the onion mechanism was only defined for Record VEOs.

These three problems are the reason why the 'Modified VEO' has been added to Version 2 of the standard.

3.5.2 Modified VEOs

A 'Modified VEO' is a type of VEO and is contained within a Signed Object (M4) element.

The Modified VEO allows the contents of a VEO to be modified. The basic mechanism is exactly the same as that used when creating an onion record. A Modified VEO contains the signed object and digital signatures from the original VEO, the object representing the revised VEO, and digital signatures to lock the two states together. Unlike an Onion VEO, a Modified VEO can contain any type of VEO; including a Record VEO, a File VEO or another Modified VEO. The latter allows for layers of modifications to be built up.

In describing how to use the Modified VEO, the expressions ‘Original Record’ and ‘Revised Record’ will be used, as these concrete terms make the description much easier to follow. However, they are slightly misleading, and readers should remember that:

- Any type of VEO may be included in a Modified VEO, not just a record.
- The ‘Original Record’ may be another Modified VEO (i.e. the record or file could already have been altered).

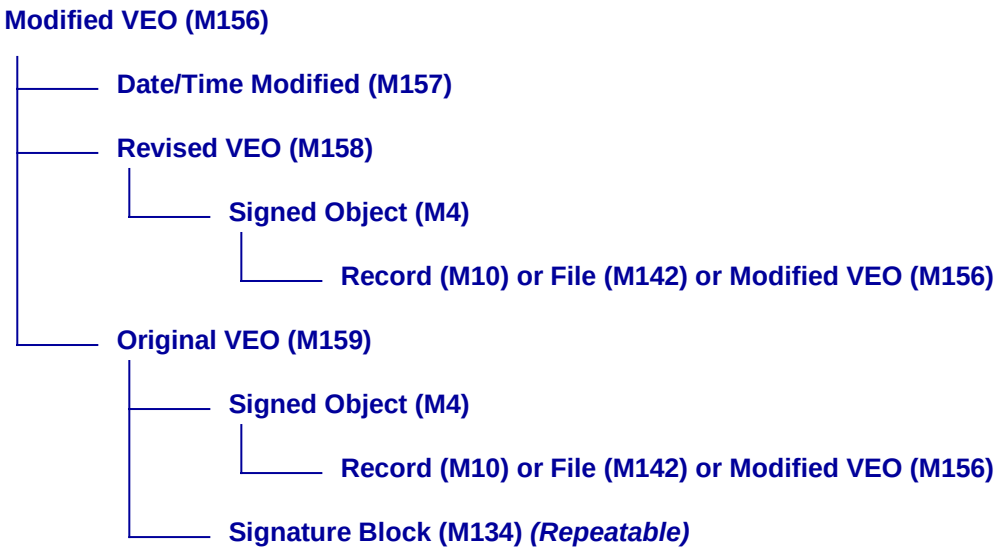


Figure 9. The general structure of a Modified VEO.

The contents of a Modified VEO are:

- *Date/Time Modified (M157).* This element contains the date and time the element was modified. It is included primarily so this information can be easily obtained when displaying the modifications to a user.
- *Revised VEO (M158).* This element contains a Signed Object containing the Revised VEO. No signature blocks are included as the integrity is preserved by the normal Signature Blocks in the VERS Encapsulated Object. Note that this element contains a ‘vers:id’ attribute which identifies this revision of the VEO.
- *Original VEO (M159).* This element contains the relevant parts of the VEO that has been modified. These parts are:

- *Signed Object (M4).* This is a copy of the original Signed Object (M4). The content of the Signed Object (M4) may be a Record VEO, a File VEO, or another Modified VEO.
- *Signature Block (M134).* These are copies of the Signature Blocks (M134).

Since the Modified VEO contains the unchanged Signed Object and Signature Blocks from the VEO that has been modified, it remains possible to verify the digital signature and hence the integrity of the record.

Note that the Original VEO element does not contain the entire original VEO. It does not contain the VEO Format Description (M2), Version (M3), or Lock Signature Block (M152) elements.

The easiest way to explain the features of a Modified VEO is to work through the process of creating a Modified VEO. In working through this process, please note:

- The Revised VEO contains all of the metadata of the VEO, not just that content which has been modified.
- The Revised VEO does not contain unmodified data files (e.g. PDF files). Instead, it contains a link to the original data buried in the Original VEO.
- The use of the Lock Signature to prevent any extraction of the Original VEO and then discarding of the Modified VEO.

Process of creating a Modified VEO

We will assume that a Record VEO is to be modified (a similar process is used for a File VEO or Modified VEO). The process of creating a Modified VEO is as follows:

1. *Check integrity of VEO.* The first step is to validate the digital signatures on the VEO, including the Lock Signature if the VEO is a Version 2 VEO. The validation of the signatures should be documented in the Management History (M66) If any of the digital signatures do not validate this should be documented, but this does not prevent modification of the VEO.

   Determining that the VEO is Version 2 must be done from examination of the Version attribute found in the Signed Object (M4) element and not by examination of the Version (M3) element. This is because the Version element is not protected by the digital signatures and hence a forger could alter the version from Version 2 to Version 1 and then remove the Lock Signature.

2. *Extract VEO contents.* Next, the Signed Object (M4) and Signature Blocks (M134) are extracted from the VEO and placed in the Original VEO (M159) element.

   Note that the Original VEO (M159) does not contain the entire VERS Encapsulated Object (in this it is unlike an ‘onion’ record). Specifically, it does not contain the VEO Format Description (M2), Version (M3), or the Lock Signature Block (M152).

3. *Construct the contents of the Revised VEO.* A copy of the original Signed Object (M4) is made and all the necessary modifications are made to it. These modifications may include:
   - Revised Record Metadata
   - Addition of a new Document
   - Removal of an existing Document
   - Modification of the Document Metadata
   - Addition of a new Encoding to a Document
   - Removal of an existing Encoding from a Document
   - Modification of the Encoding Metadata
   - Replacement of the Document Data in an Encoding

Important: When constructing a Modified VEO, a Management Event (M67) must be created in the Management History (M66) documenting the modification. The Management Event must contain:

- An Event Type (M69) of 'Record Modified' or 'Folder Modified'
- An Event Description (M70) describing why the record or folder was modified and, if possible, how the record or folder was modified. We recommend that if a small number of changes are made to a VEO these changes be listed in the Event Description. When a large number of changes are made, however, each change need not be individually listed. It would then be up to a researcher to manually compare the Original and Revised VEOs to determine the changes.

This modified copy is placed in the Revised VEO (M158) element.

Note that the Revised VEO (M158) element contains the full current state of the VEO including the elements that have not been changed. Consequently, it can be used to answer user queries without reference to earlier versions of the VEO.

Because information is duplicated, a Modified VEO is consequently large. We considered holding only those elements that had changed, but the disadvantage of this was that to view the record it would be necessary to merge all of the changes. This would not only take significant amounts of processing time for an operation that is commonly performed, but was potentially error prone. If a mistake was made in constructing the list of changed elements, for example, it would not be possible to subsequently correct the mistake.

4. *Remove unmodified copies of Encodings.* To reduce the size of the Revised VEO (M158), any Document Data (M133) that has not been changed is deleted and replaced by a reference to the original data.

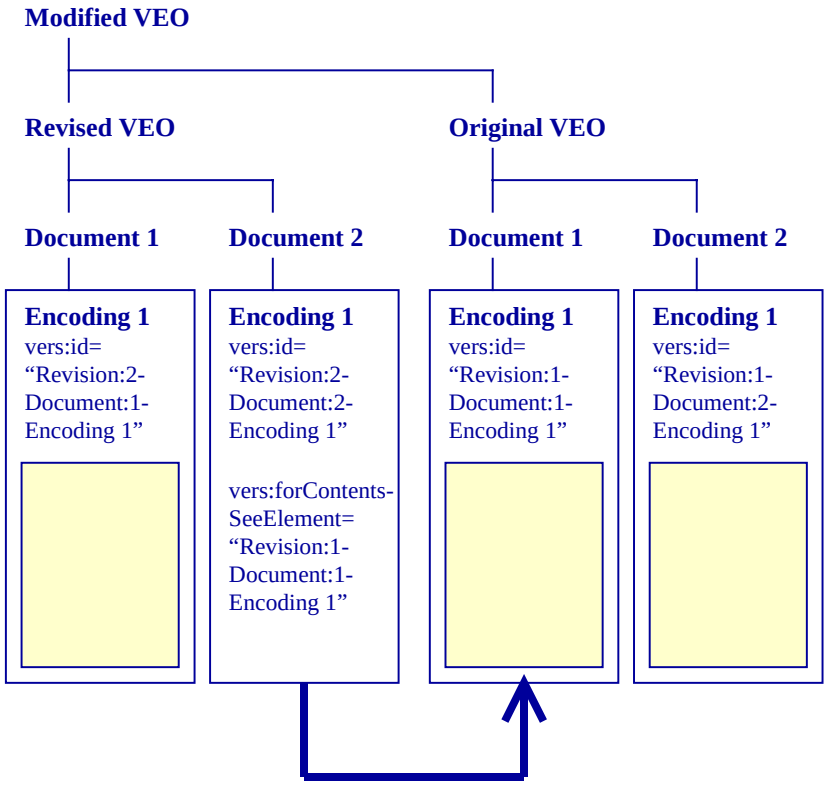


Figure 10: A Modified VEO with one Document that has not changed, one document that has been added, and one Document that has been deleted. Note that the document that has not been changed does not contain any content. Instead, it references the original copy of the document in the Original VEO.

Figure 10 shows the three possibilities for handling Documents. Revised VEO/ Document 2 is unchanged and so includes a reference to the original data instead of duplicating the data. Revised VEO/Document 1 is a new Document and so includes the full document data. Original VEO/Document 2 has been removed from the record and so does not appear in the Revised VEO (but note that the Document is still present in the VEO).

The following XML fragment shows the Modified VEO from Figure 10:

```
[...]
 <vers:SignedObject vers:VEOVersion="2.0">
 [...]
  <vers:ObjectContent>
   <vers:ModifiedVEO vers:OriginalVEOType=”Record”>
    <vers:DateTimeModified>
     2003-03-31T15:26:07-10:00
    </vers:DateTimeModified>
    <vers:RevisedVEO vers:id=”Revision:2”>
 <vers:SignedObject vers:VEOVersion="2.0">
   [...]
   <vers:Record>
    [...]
    <vers:Document vers:id="Revision:2-Document:1">
     [...]
     <vers:Encoding vers:id="Revision:2-Document:1-Encoding:1">
      [...]
      <vers:DocumentData vers:id="Revision:2-Document:1-Encoding:1-
DocumentData">
0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAEAAAAiwEAAA
[...]
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
      </vers:DocumentData>
     </vers:Encoding>
    </vers:Document>
    <vers:Document vers:id="Revision:2-Document:2">
     [...]
     <vers:Encoding vers:id="Revision:2-Document:2-Encoding:1">
      [...]
      <vers:DocumentData
        vers:id="Revision:2-Document:2-Encoding:1-DocumentData"
        vers:forContentsSeeElement="Revision:1-Document:1-Encoding:1"/>
     </vers:Encoding>
    </vers:Document>
   </vers:Record>
  </vers:ObjectContent>
 </vers:SignedObject>
    </vers:RevisedVEO>
    <vers:OriginalVEO>
     <vers:Version>2.0</vers:Version>
     [...]
 <vers:SignedObject vers:VEOVersion="2.0">
   [...]
   <vers:Record>
    [...]
    <vers:Document vers:id="Revision:1-Document:1">
     [...]
     <vers:Encoding vers:id="Revision:1-Document:1-Encoding:1">
      [...]
      <vers:DocumentData
        vers:id="Revision:1-Document:1-Encoding:1-DocumentData">
JVBERi0xLjMNJeLjz9MNCjkwIDAgb2JqDTw8IA0vTGluZWFyaXplZCAxIA0vTyA5MiANL0
[...]
JUVPRg0=
      </vers:DocumentData>
     </vers:Encoding>
    </vers:Document>
    <vers:Document vers:id="Revision:1-Document:2">
     [...]
     <vers:Encoding vers:id="Revision:1-Document:2-Encoding:1">
      [...]
```

```
      <vers:DocumentData
        vers:id="Revision:1-Document:2-Encoding:1-DocumentData"
JVBERi0xLjMNJeLjz9MNCjkwIDAgb2JqDTw8IA0vTGluZWFyaXplZCAxIA0vTyA5MiANL0
[...]
JUVPRg0=
      </vers:DocumentData>
     </vers:Encoding>
    </vers:Document>
   </vers:Record>
  </vers:ObjectContent>
 </vers:SignedObject>
    </vers:OriginalVEO>
   </vers:ModifiedVEO>
  </vers:ObjectContent>
 </vers:SignedObject>
</vers:VERSEncapsulatedObject>
```

The reference to the original Document Data is contained in an attribute in the Document Data (M133) element. The attribute depends on whether the original data was in a Version 1 VEO or a Version 2 VEO.

- *Version 2 VEO.* References to a Document Data element in a Version 2 VEO are made using the ‘vers:forContentsSeeElement’ attribute.

  A Document Data element in a Version 2 VEO must contain an vers:id attribute with the value ‘Revision:LL-Document:DD-Encoding:EE-DocumentData’ where ‘LL’ is the revision number (1 being the very first VEO, 2 being the first encapsulating ModifiedVEO, 3 being the second ModifiedVEO and so on), ‘DD’ being the number of the Document within that layer (1 being the first Document), and ‘EE’ being the number of the Encoding within that Document (1 being the first Encoding). So ‘Revision:1-Document:3-Encoding:2’ would be the second Encoding in the third Document of the original VEO.

  Note that the value of the vers:id attribute reflects the position of the Document Data element within the VEO and will change each time the VEO is encapsulated within a Modified VEO, even if the Encoding does not change. So, for example, in Figure 10 the unchanged Document is ‘Revision:1-Document:1-Encoding:1’ in the original VEO and ‘Revision:2-Document:2-Encoding:1’ in the revised VEO.
- *Version 1 VEO.* A Document Data element in a Version 1 VEO will not contain an vers:id attribute. In this case the reference is contained in a vers:forContentsSeeOriginalDocumentData attribute.

  The value of this attribute is in the same form as previously (‘Revision:LL-Document:DD-Encoding:EE’), the use of the different attribute indicating that the system must locate the relevant Document Data element itself rather than using the inbuilt XML operations.

The Document Data reference must always point directly to the element that actually contains the Document Data content (i.e. no chaining). When a VEO is modified for the second or subsequent time (i.e. when one Modified VEO encapsulates another Modified VEO) the reference in the second Modified VEO should point to the original, not to the first Modified VEO.

An example of the use of these attributes is shown on the next page.

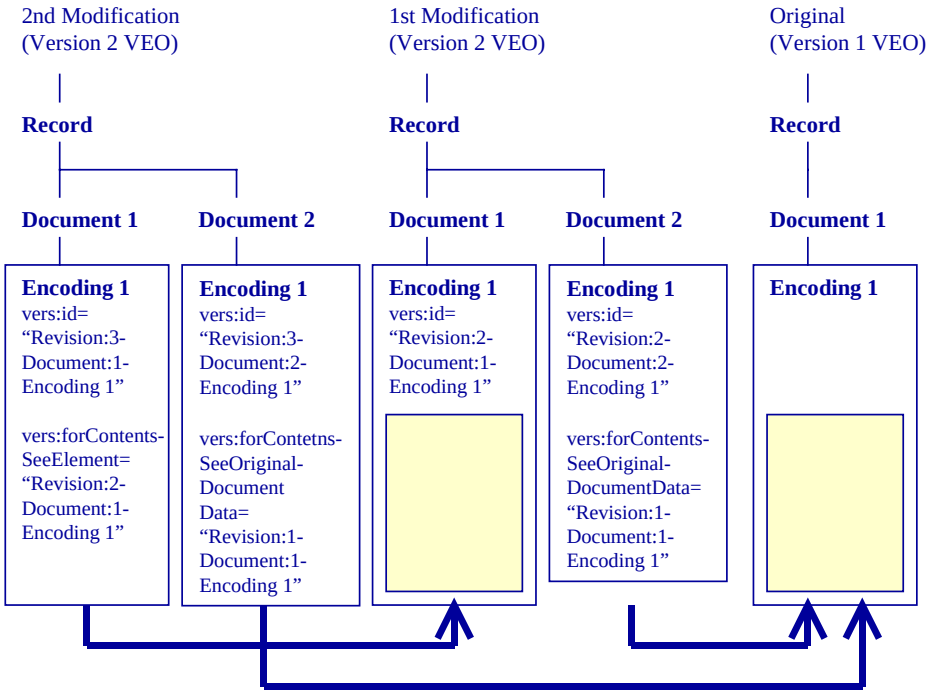


Figure 11. Sequence of modifications to a VEO showing use of vers:forContentsSeeElement and vers:forContentsSeeOriginalDocumentData attributes to refer to Version 1 and Version 2 Documents. Note that the original VEO is a Version 1 VEO, hence the references to the original Document 1 use the vers:forContentsSeeOriginalDocumentData attribute.

5. *Construct Revised VEO.* The copy of the Signed Object (made in step 3 and modified in steps 4 and 5) is inserted in a Revised VEO (M158) element. The Revised VEO element contains a 'vers:id' attribute that identifies this revision. Note that the original VEO is considered to be revision 1, and so the first revised VEO is revision 2, and so on.
6. *Construct Modified VEO.* The Revised VEO (M158) and the Original VEO (M159) elements are used to make a Modified VEO (M156) element.

   The Modified VEO element contains a vers:OriginalVEOType attribute. This contains the value 'Record' or 'Folder' depending on whether the original VEO was a record or folder. This attribute can be used by an application to determine whether a Modified VEO contains a Record VEO or a File VEO without examining the contents of the Revised VEO.

   The Modified VEO is inserted as the Signed Object in a new VEO. Finally, new Signature Blocks and a new Lock Signature are applied.

Accessing the contents of a Modified VEO

The following description gives the process for accessing information in a record (the most common case), but the process for other types of VEOs is similar.

- When it is necessary to access the metadata, it is only necessary to use the copy of the Record VEO (M10) element held inside the Revised VEO (M158) element. The Record VEO contains the current state of all the metadata.
- When it is necessary to access the content of a document, the first point of call is the latest copy of the Record VEO (M10) element held inside the Revised VEO (M158) element. If that Document or Encoding was added (or modified) in the last modification,

the actual content will be found in the Document Data (M133) element. In the more usual case, however, the Document Data (M133) will have been unchanged and will not contain any content. In this case the reference in the vers:forContentsSeeElement or vers:forContentsSeeOriginalDocumentData attributes will have to be followed to the data inside the Original VEO element.

3.5.3 Lock Signature Blocks

Lock Signature Blocks (M152) are used to prevent tampering with the record by stripping off the outermost layer of a Modified VEO and discarding the modifications. This problem affected the original 'onion' modification process (see section 3.5.1). The problem arises because the original VEO is held intact within the onion. The solution is to remove a piece of information from the original VEO when it is modified so that original VEO cannot be extracted. The information removed is the Lock Signature Block.

A Lock Signature Block (M152) only appears in a VERS Encapsulated Object. The process of applying a Lock Signature Block is as follows:

- The VEO is signed (see section 5), producing a Signature Block (M134). This signature block element contains an vers:id attribute with the value ‘Revision:LL-Signature:SS’, where ‘LL’ is the revision number (1 being the very first VEO, 2 being the first encapsulating Modified VEO, 3 being the second Modified VEO and so on), and ‘SS’ being the number of the Signature Block within that layer (1 being the first signature).
- The Signature element (M138) is then signed using the same private key used to produce the Lock Signature Block (M152) (see Figure 12). The Lock Signature Block element must contain a vers:signsSignatureBlock attribute which identifies the Signature Block containing the Signature that has been signed.

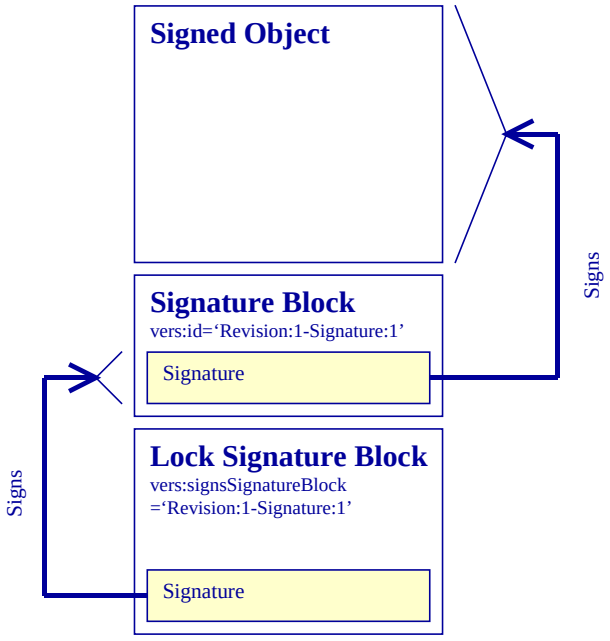


Figure 12. The signature in a Lock Signature Block signs the signature element from one of the Signature Blocks. Which Signature Block is indicated by attributes.

As described in the previous section, the Lock Signature Block is discarded when a VEO is modified and the Signed Object becomes part of the Original VEO (M159) element of a Modified VEO. To discard the outermost layer of a Modified VEO, a forger would need to recreate the Lock Signature Block. To do this, the forger requires the private key of the recordkeeping system.

Note that the use of a Lock Signature Block is not complete protection against forgery. If the forger knows, before modifying a VEO, that they will want to subsequently discard the modification, they can simply make a copy of the Lock Signature before modifying the VEO. Lock Signature Blocks will only protect the against forgers attempting to retrospectively discard modifications.

3.6 When to create a Modified VEO

Modified VEOs document changes to a record or folder. But if every change to a record or folder results in a new Modified VEO, VEOs may get very large very quickly.

It is a business decision as to how frequently changes to a record or folder are collected and a Modified VEO created. Possible decisions are:

- Every change results in the creation of a Modified VEO
- Modified VEOs are created when critical changes to the record or folder occur
- Modified VEOs are created upon demand
- Modified VEOs are created periodically (e.g. every six months)
- Modified VEOs are created upon export.

When Modified VEOs are not created upon every change to the record or folder it will be necessary to store the changes in the recordkeeping system until the Modified VEO is created.

4 Technical Introduction to VEOs

4.1 eXtensible Markup Language (XML)

The recommended long-term record format is expressed using XML 1.0 (eXtensible Markup Language). XML is a text-based markup language. XML specifications are easily extensible (unlike HTML) and are relatively simple. The XML standard is defined by the W3C.

4.1.1 Well formed versus valid VEOs

A *well formed* XML document is a valid document conforming to the syntax defined in the XML specification. A well formed document does not necessarily conform to a Document Type Definition (DTD). A *valid* XML document conforms to a Document Type Definition (DTD) and the validity constraints in the XML standard.

A VEO must be well formed and valid. The VERS DTD is referenced by the *ExternalId* of the Document Type Definition. The reference may be the URL of the official VERS DTD (currently http://www.prov.vic.gov.au/vers/published/vers.dtd) as in the following XML fragment:

```
<!DOCTYPE vers:VERSEncapsulatedObject SYSTEM
“http://www.prov.vic.gov.au/vers/published/vers.dtd”>
```

Including this URL in the *ExternalId* of a VEO will mean that a VERS implementation that uses a validating XML parser will attempt to access this site each time a VEO is accessed,

making access very slow. As an alternative, the *ExternalId* reference may be to a local copy of the VERS DTD, as in the following XML fragment:

```
<!DOCTYPE vers:VERSEncapsulatedObject SYSTEM "vers.dtd">
```

If the standard VEO defined in this specification has been extended, the definitions of the extensions must be included in the XML document type declaration *markupdecl*. Since it must always be possible to validate VEOs, any extensions must be included in the VEOs. Note that the XML standard specifies that these definitions are processed first and consequently override the standard DTD definitions. For example, the following XML declaration adds two attributes to the VERS Standard:

```
<!DOCTYPE vers:VERSEncapsulatedObject SYSTEM "vers.dtd"
[ <!ATTLIST vers:Signature dt:dt CDATA #IMPLIED>
<!ATTLIST vers:Certificate dt:dt CDATA #IMPLIED> ]>
```

4.1.2 Namespaces

VEOs extensively use two namespace: naa and vers.

- The naa namespace is used for elements defined in the NAA Recordkeeping Metadata Standard.
- The vers namespace is used for elements defined by VERS.

The URLs associated with each namespace are treated as simple names by the Namespace standard [Namespace]. According to the standard, the URLs do not need to point to a valid file and do not need to point to an XML schema. In practice, both URLs currently (December 2002) point to human-readable Web pages describing the respective metadata schemas.

An example declaration of these namespaces is:

```
<vers:VERSEncapsulatedObject
xmlns:vers="http://www.prov.vic.gov.au/gservice/standard/pros99007.htm"
xmlns:naa="http://www.naa.gov.au/recordkeeping/control/rkms/contents.html">
```

4.2 Encoding of binary objects

Any binary data in a VEO is encoded using Base64. Base64 is defined in [Base64].

Base64 is the standard mechanism used for encoding binary data for inclusion within XML. It is very widely used within the Internet, particularly with email. It encodes each 3 eight-bit bytes (24 bits) into 4 six-bit bytes. Each of the resulting 64 characters is encoded into a printable ASCII character. The encoding has the advantage of being quick and easy to encode and decode. It has the disadvantage of requiring slightly greater than 33% overhead (each 3 bytes in the binary file is converted into 4 bytes, plus there is a limit to maximum line length, so there are additional line feed characters).

5 Digital Signature Requirements

5.1 Digital signature implementation in VEOs

Unauthorised modifications to VEOs are detected using digital signatures. The digital signature covers the contents of the Signed Object (M4) element. The digital signature and

all of the information necessary to verify the signature is found in a Signature Block (M134) element. Lock Signature Blocks (M152) elements are identical in content to Signature Blocks, but are used to prevent stripping off the outermost layer of a Modified VEO (see section 3.5.3).

The calculation of a digital signature is simple when using the widely available software libraries. The trickiest part is ensuring that verification is calculated using exactly the same bit sequence that was used when the digital signature was calculated. If exactly the same bit sequence is not used the digital signature cannot be verified.

Ensuring the same bit sequence is complicated by the fact that the VEO is represented as characters in XML. Trivial changes to the VEO that do not affect its processing as XML (e.g. the addition of a space) will render the digital signature unverifiable.

Accordingly, VERS uses the following algorithm to ensure that the characters in the XML are consistently converted to a binary string. Since this algorithm was developed in the initial VERS standard, the W3C has produced a Canonicalisation Standard [Canon], which performs the same task with a great deal more rigour. The use of this canonicalisation standard in VERS is currently under consideration.

5.1.1 Selection of signed portion

The algorithm to generate the bit string to be signed or verified is as follows:

```
Open the XML file representing the VEO.
Find the '<' of the <vers:SignedObject> start tag.
For each character up to and including the '>' character of the
</vers:SignedObject> end tag.
     If the character is XML whitespace (space, Unicode U+0020, carriage
     return, Unicode U+000D; line feed, Unicode U+000A; or tab, Unicode
     U+0009)
          skip the character
     Else
          Express the character as a sequence of binary octets using UTF-8
          Add octets to the binary string
Sign or verify the resulting binary string
```

Equivalently:

- Only the contents of the Signed Object (M4) element are included in the digital signature. The characters included in the signature start from the '<' character of the <vers:SignedObject> start tag and end with the '>' of the <vers:SignedObject> end tag inclusive. Note that all characters in the XML file are included, including any comments and processing instructions.
- All XML whitespace is removed from the characters to be signed. Whitespace characters are defined as space (Unicode U+0020), carriage return (Unicode U+000D), line feed (Unicode U+000A) and tab (Unicode U+0009).
- The remaining Unicode characters are represented in binary using the UTF-8 encoding.

5.1.2 Algorithms supported

Hash Algorithms

The only hash algorithms which may be used are the SHA-1, SHA-256, and SHA-512 algorithms specified in the Secure Hash Standard [SHS]. However, hash algorithms are continually under development and subsequent versions of this standard may allow other algorithms.

Digital Signature Algorithms

Implementors have a choice of two digital signature algorithms:

- RSASSA-PKCS1-v1_5, specified in [RSA]
- DSA, specified in [DSS].

We recommend using the RSA digital signature algorithm, as this is extensively used to perform secure transactions across the Web and therefore implementations can be expected to be widely deployed and tested.

5.2 Public key storage in VERS

Validation of a digital signature requires the public key of the signer. If the public key has been lost or discarded the integrity of the preserved object cannot be verified using digital signatures. Further, verification depends on being certain that the stored public key actually belonged to the purported signer (otherwise the preserved object could be modified, resigned, and the public key replaced). Public keys must consequently be securely stored for the lifespan of the signed objects; this could be for a century or more. Note that private keys should not be archived; indeed, proof of authenticity is improved if it can be shown that private keys are destroyed once their use has ceased.

5.2.1 Obtaining public keys from a conventional Certificate Authority

In a conventional digital signature application public keys are obtained from certificates produced and stored by certificate authorities. However, it is open to question whether a certificate authority can (or should) be trusted to store the certificates it produced for the very lengthy periods of time required for preservation activities. Certificate authorities are usually commercial organisations and there is no guarantee that if the organisation fails or exits the business that the certificate store will be retained. How many commercial organisations are still in existence after 100 years? Note that there is little commercial pressure to provide cast-iron guarantees of long-term access to certificates as most digital signatures have a relatively short life.

One solution to this challenge requires an agency holding preserved digital objects to also store the necessary public keys to verify the preserved objects. The public keys would normally be held within certificates. This should not be an onerous requirement as certificates are simply digital objects and can be preserved within the same archive system that manages the actual preserved objects.

Care needs to be taken with this approach to ensure that the necessary certificates are actually captured into the system. If preserved objects are moved from one system to another the relevant certificates must be identified and moved with the preserved object. Further, custom verification software will need to be written to obtain the certificates from the archive system rather than from conventional certificate authorities. Finally, very great care needs to be taken to prevent the unauthorised addition of certificates to the system. If a forger can add certificates to the archive then they can forge or modify any preserved object (just as conventional digital signature applications such as SSL will fail if a forger can convince a user to install a fake root certificate on their computer).

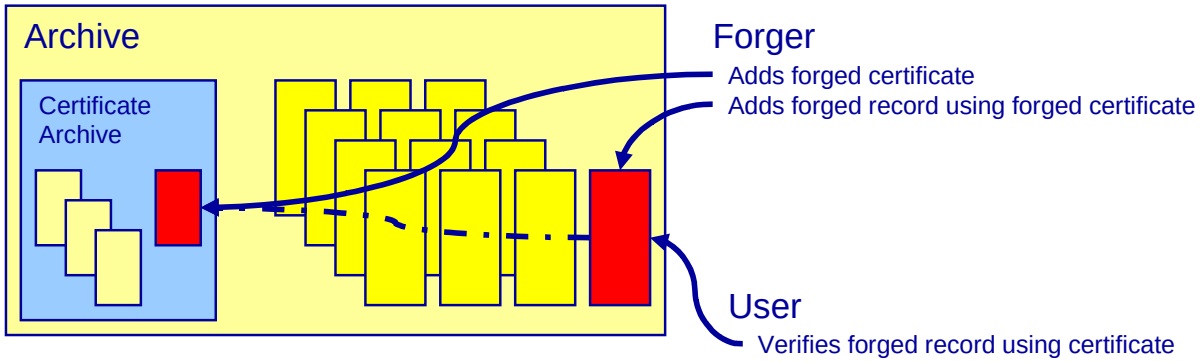


Figure 13. If a forger can add fake certificates to the archive, they can forge any records. In theory, users can detect the forgery by noticing that the certificate used to verify the signature is not the same certificate used to validate other records. In practice, users are unlikely to notice this, but VERS uses this approach as an alternative mechanism for verifying signatures.

5.2.2 Obtaining public keys from the archived record

A second option to obtaining a public key is to hold the necessary certificates within the preserved object itself. This is a particularly attractive option within VERS, as a key assumption of VERS was that preserved objects would outlive the archive system that held them so the preserved objects should stand alone from the archive system. Including the certificates within the preserved object reduces the dependency of the preserved object on other objects, ensures that the certificates are captured when the digital object is preserved, and ensure that the certificates are transferred with the preserved object. There are two problems, however. The minor problem is the inefficiency involved in storing multiple copies of certificates, though this is not serious as certificates are quite small. The major problem is that it is not secure. A little thought reveals the circular argument that you are validating the contents of a preserved object by means of a signature which, in turn, is verified by the contents of the object.

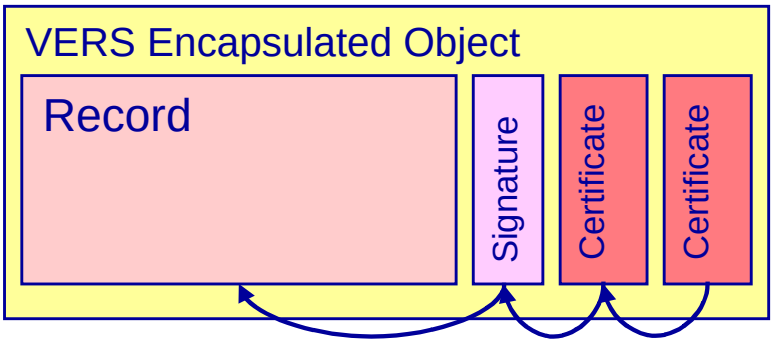


Figure 14. The VERS Encapsulated Object includes the digital signature and all of the certificates required to verify the digital signature. This makes archiving and subsequently managing the certificates trivial. This does not, however, prevent forgery as a forger can simply include their own certificates in the record.

A solution to this circular argument is to discard the conventional concept of digital signature verification by means of a certificate chain. An alternative is to adapt the process used to verify handwritten signatures in a paper-based archive. When it is necessary to verify a handwritten signature, the suspect signature is compared with other examples of the signature in the archive. If they match, the handwritten signature is treated as valid, otherwise the signature is considered suspect.

With electronic records, we compare the certificates stored with the records, not the digital signatures themselves. Clearly the digital signature will be different for each record (as the signature depends on the record). All the records signed by a user with a particular private key, however, should contain the same certificates.

When using this approach to verify the integrity of a digital signature on an electronic record, the first step is to verify the digital signature using the certificates contained in the record. This shows that the content of the record has not changed since the record was signed and that the certificates actually belong to the record. The second step is to choose another record signed by that user around that time and compare the certificates in the two records. The certificates should be identical. If they are, then either a forger has forged both records or both records are authentic. (In practice the test is slightly more involved than this, as a user's private key is periodically replaced and the certificates will validly change.) Clearly, the certificates in the suspect record should be compared with those in more than one record signed by that user; the more records compared, the more likely the records are valid. This is a probabilistic approach, but with a sufficiently large number of digital objects there would be strong evidence that the records have not been tampered with. The security can be increased further by arranging for a record to be signed multiple times.

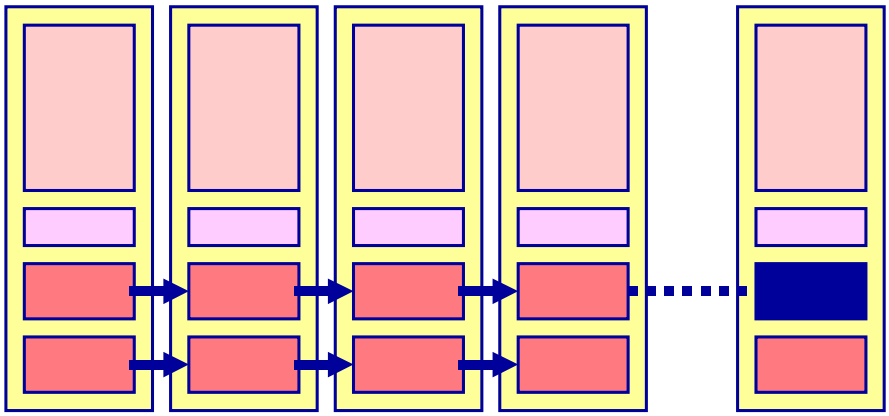


Figure 15: The four records on the left are probably valid as they were signed using the same private key; this is shown by the fact that they contain the same certificates. The record on the right is suspect as it was signed using a different private key; shown by the fact that it contains a certificate that is different to the other records in the archive.

This is a particularly useful approach as it exploits the strengths of the archive and avoids having to trust the integrity of an archive of certificates.

One useful side-effect of this 'comparison' verification is that it is possible to demonstrate when a record was created – essentially providing a notarization service. This is achieved by setting up a procedure whereby the private key used to sign the records is regularly changed, say every month. Once the private key is changed the old private key is destroyed (in fact, the copy of the private key should be destroyed once it is loaded into the system and it should not be possible to extract the private key from the system). Every record signed during that period would contain the same certificates and you can consequently show that the record must have been created in that period (as the necessary private key is not available at any other time).

The VERS Standard strongly encourages implementors to use this 'comparison' approach. As described in the next section, a VEO allows the certificate chain used to verify a signature to be stored in the VEO.

5.3 Structure of Signature Block and Lock Signature Block

A Signature Block contains one digital signature and all the information necessary to verify the signature. The structure of the Signature Block is shown in the following figure.

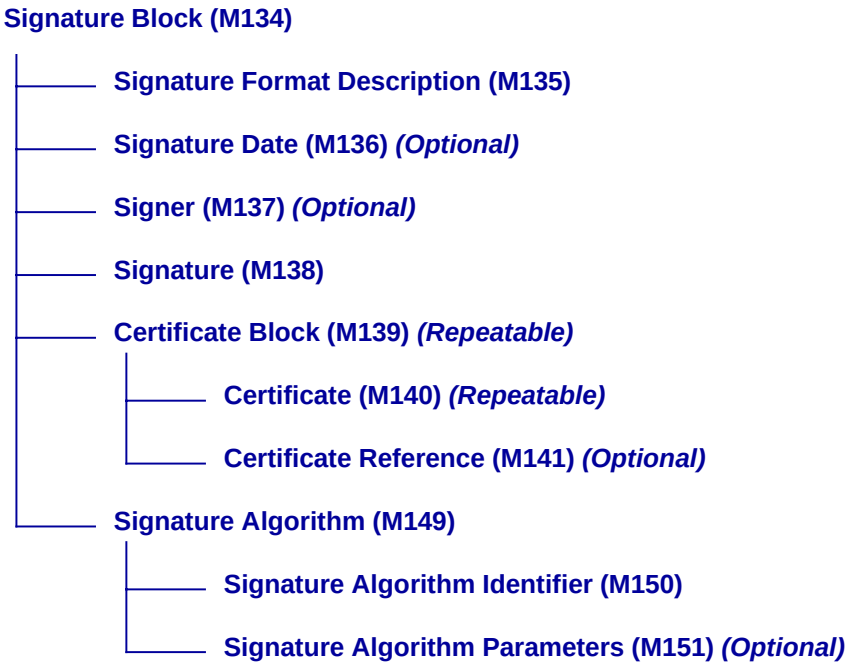


Figure 16. The contents of a Signature Block. A Lock Signature Block is identical.

The contents of the signature block are:

- *Signature Format Description* (M135). This element is a textual description of the process of generating the digital signature. It is intended to be read by developers in the future who are implementing software to verify the digital signature. Recommended values for this element are given in *PROS 99/007: Specification 2, VERS Metadata Scheme.*
- *Signature Algorithm* (M149). This element identifies the algorithms used to generate the digital signature. It is explained in more detail in section 5.3.1.
- *Signature* (M138). This element contains the actual digital signature. It is encoded in Base 64.
- *Certificate Block* (M139). This element contains the certificates necessary to verify the digital signature. This element is explained in more detail in section 5.3.2.
- *Signer* (M137) and *Signature Date* (M136). These elements are purely descriptive. They contain the name of the organisation or person who applied the digital signature, and the date the signature was applied. Note that this information is not protected by the digital signature and so cannot be trusted to be accurate.

The structure of a Lock Signature Block is identical to that of a Signature Block.

An example of a Signature Block follows:

```
<vers:SignatureBlock vers:id="Revision:1-Signature:1">
  <vers:SignatureFormatDescription>
The contents of this VEO are signed using the SHA-1 hash algorithm and the DSA
digital signature algorithm. SHA-1 is defined in Secure Hash Standard,
FIPS PUB 180-1, National Institute of Standards and Technology, US Department
of Commerce, 17 April 1995
(http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).
The DSA algorithm is defined in Digital Signature Standard (DSS), FIPS PUB
186-2, National Institute of Standards and Technology US Department of
Commerce, 27 January 2000
(http://csrc.nist.gov/publications/fips/fips186-2/fip186-2-change1.pdf).
Details of the public keys are encoded as X.509 certificates in the
vers:CertificateBlock elements. X.509 certificates are defined in "Information
technology - Open Systems Interconnection - The Directory: Public-key and
attribute certificate frameworks", ITU-T Recommendation X.509 (2000).
The signature and certificates are encoded using Base64. Base64 is defined in
Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet
Message Bodies, Section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045,
N. Freed &amp;amp; N. Borenstein, November 1996,
(http://www.ietf.org/rfc/rfc2045.txt?number=2045).
The signature covers the contents of the vers:SignedObject element starting
with the 'less than' symbol of the vers:SignedObject start tag, up to and
including the 'greater than' symbol of the vers:SignedObject end tag. Before
verifying the signature all whitespace (Unicode characters U+0009, U+000A,
U+000D, and U+0020) must be removed from the text.
  </vers:SignatureFormatDescription>
  <vers:SignatureAlgorithm>
   <vers:SignatureAlgorithmIdentifier>
1.2.840.10040.4.3
   </vers:SignatureAlgorithmIdentifier>
  </vers:SignatureAlgorithm>
  <vers:SignatureDate>2003-03-20T11:27:48-10:00</vers:SignatureDate>
  <vers:Signer>PROV Notary (Notary for PROV generated VEOs)</vers:Signer>
  <vers:Signature>
MCwCFChPTcPBV+KkuBb9YZcQEbMbfos7AhQG8yrd91Hz0D5pefIXZutJFwdHbg==
  </vers:Signature>
  <vers:CertificateBlock>
   <vers:Certificate>
MIICoTCCAmGgAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTQxNloXDTAz
MDEyMzAxNDA1NlowMjELMAkGA1UEBhMCQVUxDTALBgNVBAoTBFBST1YxFDASBgNVBAMTC1BST1Yg
Tm90YXJ5MIIBtDCCASkGByqGSM44BAEwggEcAoGA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/
gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfG
G/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFJdgUI8VIwvMspK5
gqLrhAvwWBz1AoGA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCB
gLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhR
kImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAy6h2g/EwZaGzotoIX726y32CzI1rwaNF
reYce1JvOfq94KpVqu79fQl+4tjSyxi0TS/H2RVfcdrKP+8uLTx4CQjzON2uqlvv84Lhg+Dhxc2E
JpH9RlbQa3B0RvILTjeGylcwmVUj+brdT5+foBhQHTIaeHdQsMddzJeB7QVG1cgwCQYHKoZIzjgE
AwMvADAsAhR+T7l7OSF0w9uG65gBeXGzwkMQ9AIUAvB9N2i62E9od7uDZHF1opxP0l4=
   </vers:Certificate>
   <vers:Certificate>
MIICrzCCAm+gAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTIyMVoXDTAz
MDEyMzAxMzkwMVowQDELMAkGA1UEBhMCQVUxIDAeBgNVBAoTF0RvZGd5IEJyb3MgQ2VydGlmaWNh
dGVzMQ8wDQYDVQQDEwZSb290Q0EwggG0MIIBKQYHKoZIzjgEATCCARwCgYD9f1OBHXUSKVLfSpwu
7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSf
n+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgB
xwIUl2BQjxUjC8yykrmCouuEC/BYHPUCgYD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeC
Z1FZV4661FlP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1
YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYCmx50D/58WrFwa
vjkxGr+Qq9uSQQAzte7gTOlmC1O3P6iYY5zmhZ/uWrXfieZPUK3DGyZfZ3HtG7//U+TgezgYTmyh
uiUIDzWOZlMJCU9CZrKcB5CWfqLY6ijxucMS3NedcbwgOlzVHhfcR+yqLIKh7plogBZYfQttrfSs
wuxJ0TAJBgcqhkjOOAQDAy8AMCwCFD9uWkymtSsiUriiKFEtjfXptP0rAhQ/m2+vVX+W3CpUBiH4
F8cZ5Blhyg==
   </vers:Certificate>
  </vers:CertificateBlock>
 </vers:SignatureBlock>
```

5.3.1 Indication of hash and signature algorithms

The hash and digital signature algorithms used to sign the VEO are identified by the vers:SignatureAlgorithm element. By using this element a program can automatically select the correct program to verify the signature.

The contents of this element are derived from the signature algorithm identification used in X.509 certificates.

The only element used is the Signature Algorithm Identifier (M150), as no current algorithm appears to use the Signature Algorithm Parameters (M151) element, but the element may be used if required.

The signature algorithm identifiers used are the ones used in X.509 certificates. These identify a pair of algorithms: a hash algorithm and a digital signature algorithm. The identifiers are ASN.1 Object Identifiers (OIDs) and take the form of a sequence of numbers (the identifier space forms a tree, and each number in the sequence identifies a branch in a path through the tree). OIDs have several representations. The most convenient form for mixed human and computer use is the ‘dot form’. In this form the numbers are represented textually separated, by dots: for example the string ‘1.2.840.113549.1.1.5’. There is a binary form of OIDs, but the text form is easy for computers to process and is easier for humans to read.

5.3.2 Representation of certificates

VERS uses X.509 certificates encoded using the Distinguished Encoding Rules (DER). References to the standards defining these formats are given in the Specification. A good summary of certificates and the DER encoding can be found in [RFC2459].

A Certificate Block (M139) holds a certificate chain that can be used to verify the digital signature. Since a Signature Block (M134) may contain multiple Certificate Blocks (M139), this means that a Signature Block (M134) can contain multiple certificate chains, any one of which can be used to verify the digital signature.

Each Certificate Block contains a sequence of one or more Certificate (M139) elements representing the certificate chain. Each Certificate (M139) holds a certificate. The Certificate Blocks are ordered so that:

- the first Certificate Block contains the certificate containing the signer’s public key
- the second Certificate Block contains the certificate containing the public key of the certificate authority that generated the signer’s certificate
- the last Certificate Block contains the root certificate in the certificate chain.

Only certificates necessary to verify the signature are to be included in the Signature Block.

Certificates are encoded in Base64 for inclusion in a Certificate element. Digital signature implementations will normally directly accept DER-encoded certificates, and will often accept Base64-encoded certificates.

Certificates should not be included in the encoded form used to contain a certificate and associated private key (the private key used to sign a VEO must never be included in the VEO). Examples of such formats are

- PKCS #7 (also known as a ‘.p78’ form)
- PKCS #12 (also known as a ‘.pfx’ or ‘.p12’ form)
- Microsoft Serialized Certificate Store (also known as a ‘.sst’ form).

6 Compliance with PROS 99/007 Specification 3

Compliance with PROS 99/007 requires the recordkeeping system to generate VEOs for export. More advanced levels of conformance require additional support for VEOs. This section provides guidance on the issues involved in compliance to PROS 99/007 Specification 3.

6.1 Export compliance

6.1.1 Export compliance (Version 1 systems)

The only additional requirement we are requiring of systems already compliant with Version 1 is that all VEOs must contain a digital signature. All Version 1 systems currently compliant with Specification 3 already fulfil this requirement.

6.1.2 Export compliance (Version 2 systems)

The recordkeeping system must produce VEOs that comply to this version of the Specification without any of the conditional features.

Specifically, to achieve this level of compliance Version 2 systems must produce Record VEOs that contain the following:

- At least one Signature Block (M134) (i.e. one digital signature).
- A vers:id attribute in the Signature Block element (M134); see section 3.5.3.
- A Lock Signature Block element (M152); see section 3.5.3.
- A vers:id attribute in the Document (M114), Encoding (M126), and Document Data (M133) elements.
- A vers:VEOVersion attribute in the Signed Object element (M4); see section 3.5.2.
- At least one Agent (M12).
- At least one Management Event (M67).
- At least one Document (M114) and Encoding (M126).
- At least the mandatory metadata elements:
  - VEO Format Description (M2)
  - Version (M3)
  - Signed Object (M4)
  - Object Metadata (M5)
  - Object Type (M6)
  - Object Type Description (M7)
  - Object Creation Date (M8)
  - Object Content (M9)
  - Record (M10)
  - Record Metadata (M11)
  - Agent (M12)
  - Agent Type (M13)
  - Corporate Name (M16)
  - Rights Management (M24)
  - Security Classification (M25)

  - Title (M32)
  - Scheme Type (M33)
  - Scheme Name (M34)
  - Title Words (M35)
  - Date (M54)
  - Date/Time Created (M55)
  - Date/Time Transacted (M56)
  - Date/Time Registered (M57)
  - Aggregation Level (M59)
  - Management History (M66)
  - Management Event (M67)
  - Event Date Time (M68)
  - Event Type (M69)
  - Event Description (M70)
  - Disposal (M88)
  - Disposal Authorisation (M89)
  - Sentence (M90)
  - VEO Identifier (M99)
  - Agency Identifier (M100)
  - Series Identifier (M101)
  - File Identifier (M102)
  - VERS Record Identifier (M103)
  - Document (M114)
  - Document Metadata (M115)
  - Document Agent (M116)
  - Document Title (M117)
  - Document Date (M123)
  - Document Source (M125)
  - Encoding (M126)
  - Encoding Metadata (M127)
  - File Encoding (M128)
  - File Rendering (M130)
  - Rendering Text (M131)
  - Document Data (M133)
  - Signature Block (M134)
  - Signature Format Description (M135)
  - Signature (M138)
  - Certificate Block (M139)
  - Certificate (M140)
  - Signature Algorithm (M149)
  - Signature Algorithm Identifier (M150).
- Values in the Rendering Keywords element (M132) that conform to the specification given in *PROS 99/007 Specification 2: VERS Metadata Scheme.*

Specifically, to achieve this level of compliance, Version 2 systems must produce File VEOs that contain the following:

- At least one Signature Block (M134) (i.e. one digital signature).
- A vers:id attribute in the Signature Block element (M134); see section 3.5.3.
- A Lock Signature Block element (M152); see section 3.5.3.
- A vers:VEOVersion attribute in the Signed Object element (M4); see section 3.5.2.
- At least one Agent (M12).
- At least one Management Event (M67).

- At least the mandatory metadata elements:
  - VEO Format Description (M2)
  - Version (M3)
  - Signed Object (M4)
  - Object Metadata (M5)
  - Object Type (M6)
  - Object Type Description (M7)
  - Object Creation Date (M8)
  - Object Content (M9)
  - File (M142)
  - File Metadata (M143)
  - Agent (M12)
  - Agent Type (M13)
  - Corporate Name (M16)
  - Rights Management (M24)
  - Security Classification (M25)
  - Title (M32)
  - Scheme Type (M33)
  - Scheme Name (M34)
  - Title Words (M35)
  - Date (M54)
  - Date/Time Created (M55)
  - Date/Time Transacted (M56)
  - Date/Time Registered (M57)
  - Aggregation Level (M59)
  - Management History (M66)
  - Management Event (M67)
  - Event Date Time (M68)
  - Event Type (M69)
  - Event Description (M70)
  - Disposal (M88)
  - Disposal Authorisation (M89)
  - Sentence (M90)
  - VEO Identifier (M99)
  - Agency Identifier (M100)
  - Series Identifier (M101)
  - File Identifier (M102)
  - Signature Block (M134)
  - Signature Format Description (M135)
  - Signature (M138)
  - Certificate Block (M139)
  - Certificate (M140)
  - Signature Algorithm (M149)
  - Signature Algorithm Identifier (M150).
- The values of all elements that contain dates conform to the specification given in *PROS 99/007 Specification 2: VERS Metadata Scheme,* section 14.

Systems must NOT produce VEOs that contain the following:

- Document Data elements (M133) that contain VERSEncapsulatedObject elements (M1) (i.e. onion records).

6.2 Native compliance

6.2.1 Native compliance (Version 1 systems)

The only additional requirement we are requiring of systems already compliant with Version 1 is that all VEOs must contain a digital signature. All Version 1 systems currently compliant with Specification 3 already fulfil this requirement.

We would expect that systems holding VEOs natively would also provide the ability to generate ‘onion’ records (see section 3.5.1).

6.2.2 Native compliance (Version 2 systems)

The system must produce VEOs that conform to this version of the Specification and must also be capable of producing Modified VEOs.

This level of compliance is only applicable to those systems that use the VEO internally as a native format, as these systems need to be able to modify the contents of VEOs. This level of compliance has no relevance for those systems that only produce VEOs upon export.

Specifically, to achieve this level of compliance, systems must produce VEOs that contain the following:

- All of the features required in section 6.1.2.
- The Modified VEO element (M156).
- Either a vers:forContentsSeeElement attribute or a vers:forContentsSeeOriginalDocumentAndEncoding attribute in each unmodified Document Data (M133) element.

6.3 Conditional compliance

6.3.1 Structured documents

Systems that can handle structured Documents (see section 3.4) must be capable of producing VEOs that contain the following:

- vers:id, vers:subordinateDocuments, vers:subordinateDocumentRelationship, vers:parentDocument, and vers:presentThisDocument attributes in the Document element.

6.3.2 Import compliance (Version 1)

The system must accept and handle VEOs that comply to Version 1 of this Specification. This includes the presence of digital signatures and onion VEOs.

The system must accept VEOs that contain elements and attributes in addition to those defined in Version 1 of this Specification. The system must not lose, change, or discard the information held in these elements and attributes and must be capable of subsequently exporting this information. It is not required, however, that the system use or make available information in these additional attributes.

Import-compliance does not imply native support for VEOs. A import compliant system may convert the imported VEOs into its internal data structures.

6.3.3 Import compliance (Version 2)

The system must accept and handle VEOs that comply to Version 1 of this Specification as described in section 6.3.2. This includes onion VEOs.

The system must accept and handle VEOs that comply to Version 2 of this Specification. This includes:

- Modified VEOs
- Structured documents.

Import compliance does not imply native support for VEOs. A import-compliant system may convert the imported VEOs into its internal data structures.

7 Examples of VEOs

7.1 Record VEO containing mandatory and conditional metadata

```
1    <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
2    <!DOCTYPE vers:VERSEncapsulatedObject SYSTEM "vers.dtd">
3    <vers:VERSEncapsulatedObject
4      xmlns:vers="http://www.prov.vic.gov.au/gservice/standard/pros99007.htm"
5      xmlns:naa="http://www.naa.gov.au/recordkeeping/control/rkms/contents.html">
6     <vers:VEOFormatDescription>
7      <vers:Text>
8    This record conforms to the structure defined in "Management of Electronic
9    Records, PROS 99/007 (Version 2.0)" Public Record Office Victoria, 2003.
10   The structure of this record is represented using Extensible Markup Language
11   (XML) 1.0, W3C, 1998
12     </vers:Text>
13    </vers:VEOFormatDescription>
14    <vers:Version>2.0</vers:Version>
15    <vers:SignatureBlock vers:id="Revision:1-Signature:1">
16     <vers:SignatureFormatDescription>
17   The contents of this VEO are signed using the SHA-1 hash algorithm and the DSA
18   digital signature algorithm. SHA-1 is defined in Secure Hash Standard,
19   FIPS PUB 180-1, National Institute of Standards and Technology, US Department
20   of Commerce, 17 April 1995
21   (http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).
22   The DSA algorithm is defined in Digital Signature Standard (DSS), FIPS PUB
23   186-2, National Institute of Standards and Technology US Department of
24   Commerce, 27 January 2000
25   (http://csrc.nist.gov/publications/fips/fips186-2/fip186-2-change1.pdf).
26   Details of the public keys are encoded as X.509 certificates in the
27   vers:CertificateBlock elements. X.509 certificates are defined in "Information
28   technology - Open Systems Interconnection - The Directory: Public-key and
29   attribute certificate frameworks", ITU-T Recommendation X.509 (2000).
30   The signature and certificates are encoded using Base64. Base64 is defined in
31   Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet
32   Message Bodies, Section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045,
33   N. Freed &amp;amp; N. Borenstein, November 1996,
34   (http://www.ietf.org/rfc/rfc2045.txt?number=2045).
35   The signature covers the contents of the vers:SignedObject element starting
36   with the 'less than' symbol of the vers:SignedObject start tag, up to and
37   including the 'greater than' symbol of the vers:SignedObject end tag. Before
38   verifying the signature all whitespace (Unicode characters U+0009, U+000A,
39   U+000D, and U+0020) must be removed from the text.
40     </vers:SignatureFormatDescription>
41     <vers:SignatureAlgorithm>
42      <vers:SignatureAlgorithmIdentifier>
43   1.2.840.10040.4.3
44      </vers:SignatureAlgorithmIdentifier>
45     </vers:SignatureAlgorithm>
```

```
    <vers:SignatureDate>2003-03-20T11:27:48-10:00</vers:SignatureDate>
    <vers:Signer>PROV Notary (Notary for PROV generated VEOs)</vers:Signer>
    <vers:Signature>
MCwCFChPTcPBV+KkuBb9YZcQEbMbfos7AhQG8yrd91Hz0D5pefIXZutJFwdHbg==
    </vers:Signature>
    <vers:CertificateBlock>
     <vers:Certificate>
MIICoTCCAmGgAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTQxNloXDTAz
MDEyMzAxNDA1NlowMjELMAkGA1UEBhMCQVUxDTALBgNVBAoTBFBST1YxFDASBgNVBAMTC1BST1Yg
Tm90YXJ5MIIBtDCCASkGByqGSM44BAEwggEcAoGA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/
gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfG
G/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFJdgUI8VIwvMspK5
gqLrhAvwWBz1AoGA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCB
gLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhR
kImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAy6h2g/EwZaGzotoIX726y32CzI1rwaNF
reYce1JvOfq94KpVqu79fQl+4tjSyxi0TS/H2RVfcdrKP+8uLTx4CQjzON2uqlvv84Lhg+Dhxc2E
JpH9RlbQa3B0RvILTjeGylcwmVUj+brdT5+foBhQHTIaeHdQsMddzJeB7QVG1cgwCQYHKoZIzjgE
AwMvADAsAhR+T7l7OSF0w9uG65gBeXGzwkMQ9AIUAvB9N2i62E9od7uDZHF1opxP0l4=
    </vers:Certificate>
    <vers:Certificate>
MIICrzCCAm+gAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTIyMVoXDTAz
MDEyMzAxMzkwMVowQDELMAkGA1UEBhMCQVUxIDAeBgNVBAoTF0RvZGd5IEJyb3MgQ2VydGlmaWNh
dGVzMQ8wDQYDVQQDEwZSb290Q0EwggG0MIIBKQYHKoZIzjgEATCCARwCgYD9f1OBHXUSKVLfSpwu
7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSf
n+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgB
xwIUl2BQjxUjC8yykrmCouuEC/BYHPUCgYD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeC
Z1FZV4661FlP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1
YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYCmx50D/58WrFwa
vjkxGr+Qq9uSQQAzte7gTOlmC1O3P6iYY5zmhZ/uWrXfieZPUK3DGyZfZ3HtG7//U+TgezgYTmyh
uiUIDzWOZlMJCU9CZrKcB5CWfqLY6ijxucMS3NedcbwgOlzVHhfcR+yqLIKh7plogBZYfQttrfSs
wuxJ0TAJBgcqhkjOOAQDAy8AMCwCFD9uWkymtSsiUriiKFEtjfXptP0rAhQ/m2+vVX+W3CpUBiH4
F8cZ5Blhyg==
    </vers:Certificate>
   </vers:CertificateBlock>
  </vers:SignatureBlock>
  <vers:LockSignatureBlock vers:signsSignatureBlock="Revision:1-Signature:1">
   <vers:SignatureFormatDescription>
The contents of this VEO are signed using the SHA-1 hash algorithm and the DSA
digital signature algorithm. SHA-1 is defined in Secure Hash Standard,
FIPS PUB 180-1, National Institute of Standards and Technology, US Department
of Commerce, 17 April 1995
(http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).
The DSA algorithm is defined in Digital Signature Standard (DSS), FIPS PUB
186-2, National Institute of Standards and Technology US Department of
Commerce, 27 January 2000
(http://csrc.nist.gov/publications/fips/fips186-2/fip186-2-change1.pdf).
Details of the public keys are encoded as X.509 certificates in the
vers:CertificateBlock elements. X.509 certificates are defined in "Information
technology - Open Systems Interconnection - The Directory: Public-key and
attribute certificate frameworks", ITU-T Recommendation X.509 (2000).
The signature and certificates are encoded using Base64. Base64 is defined in
Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet
Message Bodies, Section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045,
N. Freed &amp;amp; N. Borenstein, November 1996,
(http://www.ietf.org/rfc/rfc2045.txt?number=2045).
The signature covers the contents of the vers:SignedObject element starting
with the 'less than' symbol of the vers:SignedObject start tag, up to and
including the 'greater than' symbol of the vers:SignedObject end tag. Before
verifying the signature all whitespace (Unicode characters U+0009, U+000A,
U+000D, and U+0020) must be removed from the text.
   </vers:SignatureFormatDescription>
   <vers:SignatureAlgorithm>
    <vers:SignatureAlgorithmIdentifier>
1.2.840.10040.4.3
    </vers:SignatureAlgorithmIdentifier>
   </vers:SignatureAlgorithm>
   <vers:SignatureDate>2003-03-20T11:27:48-10:00</vers:SignatureDate>
   <vers:Signer>PROV Notary (Notary for PROV generated VEOs)</vers:Signer>
   <vers:Signature>
MCwCFChPTcPBV+KkuBb9YZcQEbMbfos7AhQG8yrd91Hz0D5pefIXZutJFwdHbg==
   </vers:Signature>
```

```
119     <vers:CertificateBlock>
120      <vers:Certificate>
121   MIICoTCCAmGgAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
122   eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTQxNloXDTAz
123   MDEyMzAxNDA1NlowMjELMAkGA1UEBhMCQVUxDTALBgNVBAoTBFBST1YxFDASBgNVBAMTC1BST1Yg
124   Tm90YXJ5MIIBtDCCASkGByqGSM44BAEwggEcAoGA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/
125   gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfG
126   G/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFJdgUI8VIwvMspK5
127   gqLrhAvwWBz1AoGA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCB
128   gLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhR
129   kImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAy6h2g/EwZaGzotoIX726y32CzI1rwaNF
130   reYce1JvOfq94KpVqu79fQl+4tjSyxi0TS/H2RVfcdrKP+8uLTx4CQjzON2uqlvv84Lhg+Dhxc2E
131   JpH9RlbQa3B0RvILTjeGylcwmVUj+brdT5+foBhQHTIaeHdQsMddzJeB7QVG1cgwCQYHKoZIzjgE
132   AwMvADAsAhR+T7l7OSF0w9uG65gBeXGzwkMQ9AIUAvB9N2i62E9od7uDZHF1opxP0l4=
133      </vers:Certificate>
134      <vers:Certificate>
135   MIICrzCCAm+gAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
136   eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTIyMVoXDTAz
137   MDEyMzAxMzkwMVowQDELMAkGA1UEBhMCQVUxIDAeBgNVBAoTF0RvZGd5IEJyb3MgQ2VydGlmaWNh
138   dGVzMQ8wDQYDVQQDEwZSb290Q0EwggG0MIIBKQYHKoZIzjgEATCCARwCgYD9f1OBHXUSKVLfSpwu
139   7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSf
140   n+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgB
141   xwIUl2BQjxUjC8yykrmCouuEC/BYHPUCgYD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeC
142   Z1FZV4661FlP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1
143   YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYCmx50D/58WrFwa
144   vjkxGr+Qq9uSQQAzte7gTOlmC1O3P6iYY5zmhZ/uWrXfieZPUK3DGyZfZ3HtG7//U+TgezgYTmyh
145   uiUIDzWOZlMJCU9CZrKcB5CWfqLY6ijxucMS3NedcbwgOlzVHhfcR+yqLIKh7plogBZYfQttrfSs
146   wuxJ0TAJBgcqhkjOOAQDAy8AMCwCFD9uWkymtSsiUriiKFEtjfXptP0rAhQ/m2+vVX+W3CpUBiH4
147   F8cZ5Blhyg==
148      </vers:Certificate>
149     </vers:CertificateBlock>
150    </vers:LockSignatureBlock>
151    <vers:SignedObject vers:VEOVersion="2.0">
152     <vers:ObjectMetadata>
153      <vers:ObjectType>Record</vers:ObjectType>
154      <vers:ObjectTypeDescription>
155   This object contains a record; that is a collection of information
156   that must be preserved for a period of time.
157      </vers:ObjectTypeDescription>
158      <vers:ObjectCreationDate>2003-03-20T11:27:40-
       10:00</vers:ObjectCreationDate>
159     </vers:ObjectMetadata>
160     <vers:ObjectContent>
161      <vers:Record>
162       <vers:RecordMetadata>
163        <naa:Agent>
164         <naa:AgentType>
165          Document Author
166         </naa:AgentType>
167         <naa:Jurisdiction>
168          Victoria
169         </naa:Jurisdiction>
170         <naa:CorporateId>
171          VA 683
172         </naa:CorporateId>
173         <naa:CorporateName>
174          Public Record Office Victoria
175         </naa:CorporateName>
176        </naa:Agent>
177        <naa:RightsManagement>
178         <naa:SecurityClassification>
179          Unclassified
180         </naa:SecurityClassification>
181         <naa:UsageCondition>
182          Copyright State of Victoria 2000
183         </naa:UsageCondition>
184        </naa:RightsManagement>
185        <naa:Title>
186         <naa:SchemeType>
187          Free text
188         </naa:SchemeType>
189         <naa:SchemeName>
190          None
```

```
191         </naa:SchemeName>
192         <naa:TitleWords>
193          Integrity of Government Information, The VERS Experience
194         </naa:TitleWords>
195        </naa:Title>
196        <naa:Language>
197         en
198        </naa:Language>
199        <naa:Date>
200         <naa:DateTimeCreated>
201          2003-03-20T23:26:07-10:00
202         </naa:DateTimeCreated>
203         <naa:DateTimeTransacted>
204          2003-03-20T23:26:07-10:00
205         </naa:DateTimeTransacted>
206         <naa:DateTimeRegistered>
207          2003-03-20T23:26:07-10:00
208         </naa:DateTimeRegistered>
209        </naa:Date>
210        <naa:AggregationLevel>
211         Item
212        </naa:AggregationLevel>
213        <naa:ManagementHistory>
214         <vers:ManagementEvent>
215          <naa:EventDateTime>
216           2003-03-20T23:26:12-10:00
217          </naa:EventDateTime>
218          <naa:EventType>
219           Created
220          </naa:EventType>
221          <naa:EventDescription>
222           Created by user rkm (Rowan McKenzie)
223          </naa:EventDescription>
224         </vers:ManagementEvent>
225         <vers:ManagementEvent>
226          <naa:EventDateTime>
227           2003-03-27T23:26:12-10:00
228          </naa:EventDateTime>
229          <naa:EventType>
230           Custody Transferred
231          </naa:EventType>
232          <naa:EventDescription>
233           Encapsulated in VERS format and exported from EMPS system to
234           VERS system
235          </naa:EventDescription>
236         </vers:ManagementEvent>
237        </naa:ManagementHistory>
238        <naa:Disposal>
239         <naa:DisposalAuthorisation>
240          No Disposal Coverage
241         </naa:DisposalAuthorisation>
242         <naa:Sentence>
243          No Disposal Coverage
244         </naa:Sentence>
245         <naa:DisposalActionDue>
246          Null
247         </naa:DisposalActionDue>
248         <naa:DisposalStatus>
249          Unknown
250         </naa:DisposalStatus>
251        </naa:Disposal>
252        <vers:VEOIdentifier>
253         <vers:FileIdentifier>
254          <vers:Text>
255           99/876
256          </vers:Text>
257         </vers:FileIdentifier>
258         <vers:VERSRecordIdentifier>
259          <vers:Text>
260           11234
261          </vers:Text>
262         </vers:VERSRecordIdentifier>
263        </vers:VEOIdentifier>
```

```
264      </vers:RecordMetadata>
265      <vers:Document vers:id="Revision:1-Document:1">
266       <vers:DocumentMetadata>
267        <vers:DocumentAgent>
268         <vers:Text>
269          Author: Andrew Waugh
270         </vers:Text>
271        </vers:DocumentAgent>
272        <vers:DocumentTitle>
273         <vers:Text>
274          Report
275         </vers:Text>
276        </vers:DocumentTitle>
277        <vers:DocumentDate>
278         <vers:Text>
279          2003-03-20T23:24:06-10:00
280         </vers:Text>
281        </vers:DocumentDate>
282        <vers:DocumentSource>
283         <vers:Text>
284          Microsoft Word 97
285         </vers:Text>
286        </vers:DocumentSource>
287       </vers:DocumentMetadata>
288       <vers:Encoding vers:id="Revision:1-Document:1-Encoding:1">
289        <vers:EncodingMetadata>
290         <vers:FileEncoding>
291          <vers:Text>
292  The content of the DocumentData element is a PDF file. The file conforms to
293  'PDF Reference', third edition, Adobe Portable Document Format, Version 1.4,
294  Adobe Systems Incorporated, Addison Wesley, 2001, ISBN 0-201-75839-3
295  (http://partners.adobe.com/asn/developer/acrosdk/docs/filefmtspecs/PDFReferenc
       e.pdf
296  visited 7 January 2003) as modified in the 'Errata for PDF Reference, third
297  edition' (http://partners.adobe.com/asn/developer/acrosdk/docs/PDF14errata.txt
298  visited 7 January 2003). It may contain digital signatures defined by PDF
299  Public-key Digital Signature and Encryption Specification, Version 3.2, Jim
300  Pravetz, 12 September 2001, Adobe Systems Incorporated
301  (http://partners.adobe.com/asn/developer/pdfs/tn/ppk_pdfspec.pdf visited
302  28 March 2003) and the appearance of the digital signature in a PDF document
303  is defined in Digital Signature Appearances for Public-Key Interoperability,
304  Adobe Systems Incorporated, September 2001
305  (http://partners.adobe.com/asn/developer/pdfs/tn/PPKAppearances.pdf visited
306  28 March 2003). The file has been encoded using Base64 which is defined in
307  IETF RFC 2045 "Multipurpose Internet Mail Extensions (MIME) Part One:
308  Format of Internet Message Bodies", Section 6.8
309  "Base64 Content-Transfer-Encoding".
310          </vers:Text>
311         </vers:FileEncoding>
312         <vers:SourceFileIdentifier>
313          P:\Presentations\PublicAccountsCtee\VERSIntegrity.pdf
314         </vers:SourceFileIdentifier>
315         <vers:FileRendering>
316          <vers:RenderingText>
317           <vers:Text>
318            See the vers:FileEncoding element
319           </vers:Text>
320          </vers:RenderingText>
321          <vers:RenderingKeywords>
322           b64 pdf
323          </vers:RenderingKeywords>
324         </vers:FileRendering>
325        </vers:EncodingMetadata>
326        <vers:DocumentData
327          vers:id="Revision:1-Document:1-Encoding:1-DocumentData">
328  JVBERi0xLjMNJeLjz9MNCjkwIDAgb2JqDTw8IA0vTGluZWFyaXplZCAxIA0vTyA5MiANL0ggWyAx
329  [...]
330  MGQ+PDJjNWViMzQ4YjcyNzU3ZGUxODRjMTVjYTVjMjA2YWRhPl0NPj4Nc3RhcnR4cmVmDTE3Mw0l
331  JUVPRg0=
332       </vers:DocumentData>
333      </vers:Encoding>
334     </vers:Document>
335    </vers:Record>
```

```
336     </vers:ObjectContent>
337    </vers:SignedObject>
338   </vers:VERSEncapsulatedObject>
```

7.2 Record VEO containing optional metadata

```
1     <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
2     <!DOCTYPE vers:VERSEncapsulatedObject SYSTEM "vers.dtd">
3     <vers:VERSEncapsulatedObject
4       xmlns:vers="http://www.prov.vic.gov.au/gservice/standard/pros99007.htm"
5       xmlns:naa="http://www.naa.gov.au/recordkeeping/control/rkms/contents.html">
6      <vers:VEOFormatDescription>
7       <vers:Text>
8     This record conforms to the structure defined in "Management of Electronic
9     Records, PROS 99/007 (Version 2.0)" Public Record Office Victoria, 2003.
10    The structure of this record is represented using Extensible Markup Language
11    (XML) 1.0, W3C, 1998.
12      </vers:Text>
13     </vers:VEOFormatDescription>
14     <vers:Version>2.0</vers:Version>
15     <vers:SignatureBlock vers:id="Revision:1-Signature:1">
16      <vers:SignatureFormatDescription>
17    The contents of this VEO are signed using the SHA-1 hash algorithm and the DSA
18    digital signature algorithm. SHA-1 is defined in Secure Hash Standard,
19    FIPS PUB 180-1, National Institute of Standards and Technology, US Department
20    of Commerce, 17 April 1995
21    (http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).
22    The DSA algorithm is defined in Digital Signature Standard (DSS), FIPS PUB
23    186-2, National Institute of Standards and Technology US Department of
24    Commerce, 27 January 2000
25    (http://csrc.nist.gov/publications/fips/fips186-2/fip186-2-change1.pdf).
26    Details of the public keys are encoded as X.509 certificates in the
27    vers:CertificateBlock elements. X.509 certificates are defined in "Information
28    technology - Open Systems Interconnection - The Directory: Public-key and
29    attribute certificate frameworks", ITU-T Recommendation X.509 (2000).
30    The signature and certificates are encoded using Base64. Base64 is defined in
31    Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet
32    Message Bodies, Section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045,
33    N. Freed &amp;amp; N. Borenstein, November 1996,
34    (http://www.ietf.org/rfc/rfc2045.txt?number=2045).
35    The signature covers the contents of the vers:SignedObject element starting
36    with the 'less than' symbol of the vers:SignedObject start tag, up to and
37    including the 'greater than' symbol of the vers:SignedObject end tag. Before
38    verifying the signature all whitespace (Unicode characters U+0009, U+000A,
39    U+000D, and U+0020) must be removed from the text.
40      </vers:SignatureFormatDescription>
41      <vers:SignatureAlgorithm>
42       <vers:SignatureAlgorithmIdentifier>
43    1.2.840.10040.4.3
44       </vers:SignatureAlgorithmIdentifier>
45      </vers:SignatureAlgorithm>
46      <vers:SignatureDate>2003-03-30T05:04:25-10:00</vers:SignatureDate>
47      <vers:Signer>PROV Notary (Notary for PROV generated VEOs)</vers:Signer>
48      <vers:Signature>
49    MCwCFDEkcxNAD23bVijId7BddMqDbograhQS336tarMu3kec3gpfGQa4uc+m6g==
50      </vers:Signature>
51      <vers:CertificateBlock>
52       <vers:Certificate>
53    MIICoTCCAmGgAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
54    eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTQxNloXDTAz
55    MDEyMzAxNDA1NlowMjELMAkGA1UEBhMCQVUxDTALBgNVBAoTBFBST1YxFDASBgNVBAMTC1BST1Yg
56    Tm90YXJ5MIIBtDCCASkGByqGSM44BAEwggEcAoGA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/
57    gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfG
58    G/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFJdgUI8VIwvMspK5
59    gqLrhAvwWBz1AoGA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCB
60    gLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhR
61    kImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAy6h2g/EwZaGzotoIX726y32CzI1rwaNF
62    reYce1JvOfq94KpVqu79fQl+4tjSyxi0TS/H2RVfcdrKP+8uLTx4CQjzON2uqlvv84Lhg+Dhxc2E
63    JpH9RlbQa3B0RvILTjeGylcwmVUj+brdT5+foBhQHTIaeHdQsMddzJeB7QVG1cgwCQYHKoZIzjgE
64    AwMvADAsAhR+T7l7OSF0w9uG65gBeXGzwkMQ9AIUAvB9N2i62E9od7uDZHF1opxP0l4=
65       </vers:Certificate>
```

```
66      <vers:Certificate>
67    MIICrzCCAm+gAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
68    eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTIyMVoXDTAz
69    MDEyMzAxMzkwMVowQDELMAkGA1UEBhMCQVUxIDAeBgNVBAoTF0RvZGd5IEJyb3MgQ2VydGlmaWNh
70    dGVzMQ8wDQYDVQQDEwZSb290Q0EwggG0MIIBKQYHKoZIzjgEATCCARwCgYD9f1OBHXUSKVLfSpwu
71    7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSf
72    n+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgB
73    xwIUl2BQjxUjC8yykrmCouuEC/BYHPUCgYD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeC
74    Z1FZV4661FlP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1
75    YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYCmx50D/58WrFwa
76    vjkxGr+Qq9uSQQAzte7gTOlmC1O3P6iYY5zmhZ/uWrXfieZPUK3DGyZfZ3HtG7//U+TgezgYTmyh
77    uiUIDzWOZlMJCU9CZrKcB5CWfqLY6ijxucMS3NedcbwgOlzVHhfcR+yqLIKh7plogBZYfQttrfSs
78    wuxJ0TAJBgcqhkjOOAQDAy8AMCwCFD9uWkymtSsiUriiKFEtjfXptP0rAhQ/m2+vVX+W3CpUBiH4
79    F8cZ5Blhyg==
80      </vers:Certificate>
81    </vers:CertificateBlock>
82   </vers:SignatureBlock>
83   <vers:LockSignatureBlock vers:signsSignatureBlock="Revision:1-Signature:1">
84    <vers:SignatureFormatDescription>
85    The contents of this VEO are signed using the SHA-1 hash algorithm and the DSA
86    digital signature algorithm. SHA-1 is defined in Secure Hash Standard,
87    FIPS PUB 180-1, National Institute of Standards and Technology, US Department
88    of Commerce, 17 April 1995
89    (http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).
90    The DSA algorithm is defined in Digital Signature Standard (DSS), FIPS PUB
91    186-2, National Institute of Standards and Technology US Department of
92    Commerce, 27 January 2000
93    (http://csrc.nist.gov/publications/fips/fips186-2/fip186-2-change1.pdf).
94    Details of the public keys are encoded as X.509 certificates in the
95    vers:CertificateBlock elements. X.509 certificates are defined in "Information
96    technology - Open Systems Interconnection - The Directory: Public-key and
97    attribute certificate frameworks", ITU-T Recommendation X.509 (2000).
98    The signature and certificates are encoded using Base64. Base64 is defined in
99    Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet
100   Message Bodies, Section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045,
101   N. Freed &amp;amp; N. Borenstein, November 1996,
102   (http://www.ietf.org/rfc/rfc2045.txt?number=2045).
103   The signature covers the contents of the vers:SignedObject element starting
104   with the 'less than' symbol of the vers:SignedObject start tag, up to and
105   including the 'greater than' symbol of the vers:SignedObject end tag. Before
106   verifying the signature all whitespace (Unicode characters U+0009, U+000A,
107   U+000D, and U+0020) must be removed from the text.
108     </vers:SignatureFormatDescription>
109     <vers:SignatureAlgorithm>
110      <vers:SignatureAlgorithmIdentifier>
111   1.2.840.10040.4.3
112      </vers:SignatureAlgorithmIdentifier>
113     </vers:SignatureAlgorithm>
114     <vers:SignatureDate>2003-03-30T05:04:25-10:00</vers:SignatureDate>
115     <vers:Signer>PROV Notary (Notary for PROV generated VEOs)</vers:Signer>
116     <vers:Signature>
117   MCwCFDEkcxNAD23bVijId7BddMqDbograhQS336tarMu3kec3gpfGQa4uc+m6g==
118     </vers:Signature>
119     <vers:CertificateBlock>
120      <vers:Certificate>
121   MIICoTCCAmGgAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
122   eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTQxNloXDTAz
123   MDEyMzAxNDA1NlowMjELMAkGA1UEBhMCQVUxDTALBgNVBAoTBFBST1YxFDASBgNVBAMTC1BST1Yg
124   Tm90YXJ5MIIBtDCCASkGByqGSM44BAEwggEcAoGA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/
125   gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfG
126   G/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFJdgUI8VIwvMspK5
127   gqLrhAvwWBz1AoGA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCB
128   gLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhR
129   kImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAy6h2g/EwZaGzotoIX726y32CzI1rwaNF
130   reYce1JvOfq94KpVqu79fQl+4tjSyxi0TS/H2RVfcdrKP+8uLTx4CQjzON2uqlvv84Lhg+Dhxc2E
131   JpH9RlbQa3B0RvILTjeGylcwmVUj+brdT5+foBhQHTIaeHdQsMddzJeB7QVG1cgwCQYHKoZIzjgE
132   AwMvADAsAhR+T7l7OSF0w9uG65gBeXGzwkMQ9AIUAvB9N2i62E9od7uDZHF1opxP0l4=
133      </vers:Certificate>
134      <vers:Certificate>
135   MIICrzCCAm+gAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
136   eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTIyMVoXDTAz
137   MDEyMzAxMzkwMVowQDELMAkGA1UEBhMCQVUxIDAeBgNVBAoTF0RvZGd5IEJyb3MgQ2VydGlmaWNh
138   dGVzMQ8wDQYDVQQDEwZSb290Q0EwggG0MIIBKQYHKoZIzjgEATCCARwCgYD9f1OBHXUSKVLfSpwu
```

```
7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSf
n+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgB
xwIUl2BQjxUjC8yykrmCouuEC/BYHPUCgYD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeC
Z1FZV4661FlP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1
YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYCmx50D/58WrFwa
vjkxGr+Qq9uSQQAzte7gTOlmC1O3P6iYY5zmhZ/uWrXfieZPUK3DGyZfZ3HtG7//U+TgezgYTmyh
uiUIDzWOZlMJCU9CZrKcB5CWfqLY6ijxucMS3NedcbwgOlzVHhfcR+yqLIKh7plogBZYfQttrfSs
wuxJ0TAJBgcqhkjOOAQDAy8AMCwCFD9uWkymtSsiUriiKFEtjfXptP0rAhQ/m2+vVX+W3CpUBiH4
F8cZ5Blhyg==
   </vers:Certificate>
  </vers:CertificateBlock>
 </vers:LockSignatureBlock>
 <vers:SignedObject vers:VEOVersion="2.0">
  <vers:ObjectMetadata>
   <vers:ObjectType>Record</vers:ObjectType>
   <vers:ObjectTypeDescription>
This object contains a record; that is a collection of information
that must be preserved for a period of time.
   </vers:ObjectTypeDescription>
   <vers:ObjectCreationDate>2003-03-30T05:04:10-
    10:00</vers:ObjectCreationDate>
  </vers:ObjectMetadata>
  <vers:ObjectContent>
   <vers:Record>
    <vers:RecordMetadata>
     <naa:Agent>
      <naa:AgentType>
       Document Author
      </naa:AgentType>
      <naa:Jurisdiction>
       Victoria
      </naa:Jurisdiction>
      <naa:CorporateId>
       VA 654
      </naa:CorporateId>
      <naa:CorporateName>
       Public Record Office Victoria
      </naa:CorporateName>
     </naa:Agent>
     <naa:Agent>
      <naa:AgentType>
       Registrar
      </naa:AgentType>
      <naa:Jurisdiction>
       Victoria
      </naa:Jurisdiction>
      <naa:CorporateId>
       VA 654
      </naa:CorporateId>
      <naa:CorporateName>
       Public Record Office Victoria
      </naa:CorporateName>
      <naa:PersonalName>
       John Smith
      </naa:PersonalName>
      <naa:SectionName>
       VERS Centre of Excellence
      </naa:SectionName>
      <naa:PositionName>
       Technical Research Manager
      </naa:PositionName>
      <naa:ContactDetails>
       PO Box 2100 North Melbourne Victoria 3051 Australia
      </naa:ContactDetails>
      <naa:Email>
       John.Smith@dpc.prov.vic.gov.au
      </naa:Email>
     </naa:Agent>
     <naa:RightsManagement>
      <naa:SecurityClassification>
       Unclassified
      </naa:SecurityClassification>
      <naa:UsageCondition>
```

```
211          Copyright State of Victoria 2000
212         </naa:UsageCondition>
213        </naa:RightsManagement>
214        <naa:Title>
215         <naa:SchemeType>
216          Free text
217         </naa:SchemeType>
218         <naa:SchemeName>
219          None
220         </naa:SchemeName>
221         <naa:TitleWords>
222          Management of Electronic Records
223         </naa:TitleWords>
224         <naa:Alternative>
225          PROS 99/007
226         </naa:Alternative>
227         <naa:Alternative>
228          Victorian Electronic Records Strategy (VERS)
229         </naa:Alternative>
230        </naa:Title>
231        <naa:Description>
232         This is part of the VERS standard.
233        </naa:Description>
234        <naa:Language>
235         en
236        </naa:Language>
237        <naa:Relation>
238         <naa:RelatedItemId>
239          <vers:VEOIdentifier>
240           <vers:FileIdentifier>
241            <vers:Text>
242             99-89
243            </vers:Text>
244           </vers:FileIdentifier>
245           <vers:VERSRecordIdentifier>
246            <vers:Text>
247             100
248            </vers:Text>
249           </vers:VERSRecordIdentifier>
250          </vers:VEOIdentifier>
251         </naa:RelatedItemId>
252         <naa:RelationType>
253          Replaces
254         </naa:RelationType>
255         <naa:RelationDescription>
256          Replaced with new version
257         </naa:RelationDescription>
258        </naa:Relation>
259        <naa:Date>
260         <naa:DateTimeCreated>
261          2003-03-30T05:02:17-10:00
262         </naa:DateTimeCreated>
263         <naa:DateTimeTransacted>
264          2003-03-30T05:02:17-10:00
265         </naa:DateTimeTransacted>
266         <naa:DateTimeRegistered>
267          2003-03-30T05:02:17-10:00
268         </naa:DateTimeRegistered>
269        </naa:Date>
270        <naa:AggregationLevel>
271         Item
272        </naa:AggregationLevel>
273        <naa:ManagementHistory>
274         <vers:ManagementEvent>
275          <naa:EventDateTime>
276           2003-03-30T05:02:38-10:00
277          </naa:EventDateTime>
278          <naa:EventType>
279           Created
280          </naa:EventType>
281          <naa:EventDescription>
282           Created by John Smith
283          </naa:EventDescription>
```

```
284         </vers:ManagementEvent>
285        </naa:ManagementHistory>
286        <naa:Disposal>
287         <naa:DisposalAuthorisation>
288          No Disposal Coverage
289         </naa:DisposalAuthorisation>
290         <naa:Sentence>
291          No Disposal Coverage
292         </naa:Sentence>
293         <naa:DisposalActionDue>
294          Null
295         </naa:DisposalActionDue>
296         <naa:DisposalStatus>
297          Unknown
298         </naa:DisposalStatus>
299        </naa:Disposal>
300        <vers:VEOIdentifier>
301         <vers:AgencyIdentifier>
302          <vers:Text>
303           VA 654
304          </vers:Text>
305         </vers:AgencyIdentifier>
306         <vers:SeriesIdentifier>
307          <vers:Text>
308           1123
309          </vers:Text>
310         </vers:SeriesIdentifier>
311         <vers:FileIdentifier>
312          <vers:Text>
313           99-89
314          </vers:Text>
315         </vers:FileIdentifier>
316         <vers:VERSRecordIdentifier>
317          <vers:Text>
318           100
319          </vers:Text>
320         </vers:VERSRecordIdentifier>
321        </vers:VEOIdentifier>
322       </vers:RecordMetadata>
323       <vers:Document vers:id="Revision:1-Document:1">
324        <vers:DocumentMetadata>
325         <vers:DocumentAgent>
326          <vers:Text>
327           Author: Public Record Office Victoria
328          </vers:Text>
329         </vers:DocumentAgent>
330         <vers:DocumentTitle>
331          <vers:Text>
332           Standard
333          </vers:Text>
334         </vers:DocumentTitle>
335         <vers:DocumentDate>
336          <vers:Text>
337           2003-03-30T04:58:31-10:00
338          </vers:Text>
339         </vers:DocumentDate>
340         <vers:DocumentSource>
341          <vers:Text>
342           Microsoft Word 97 (Version 8)
343          </vers:Text>
344         </vers:DocumentSource>
345        </vers:DocumentMetadata>
346        <vers:Encoding vers:id="Revision:1-Document:1-Encoding:1">
347         <vers:EncodingMetadata>
348          <vers:FileEncoding>
349           <vers:Text>
350  The content of the DocumentData element is a PDF file. The file conforms to
351  'PDF Reference', third edition, Adobe Portable Document Format, Version 1.4,
352  Adobe Systems Incorporated, Addison Wesley, 2001, ISBN 0-201-75839-3
353  (http://partners.adobe.com/asn/developer/acrosdk/docs/filefmtspecs/PDFReference.pdf
354  visited 7 January 2003) as modified in the 'Errata for PDF Reference, third
355  edition' (http://partners.adobe.com/asn/developer/acrosdk/docs/PDF14errata.txt
```

```
visited 7 January 2003). It may contain digital signatures defined by PDF
Public-key Digital Signature and Encryption Specification, Version 3.2, Jim
Pravetz, 12 September 2001, Adobe Systems Incorporated
(http://partners.adobe.com/asn/developer/pdfs/tn/ppk_pdfspec.pdf visited
28 March 2003) and the appearance of the digital signature in a PDF document
is defined in Digital Signature Appearances for Public-Key Interoperability,
Adobe Systems Incorporated, September 2001
(http://partners.adobe.com/asn/developer/pdfs/tn/PPKAppearances.pdf visited
28 March 2003). The file has been encoded using Base64 which is defined in
IETF RFC 2045 “Multipurpose Internet Mail Extensions (MIME) Part One:
Format of Internet Message Bodies”, Section 6.8
“Base64 Content-Transfer-Encoding”.
        </vers:Text>
       </vers:FileEncoding>
       <vers:SourceFileIdentifier>
        O:\E-RECORD\VERS (97-102)\Standard (99-89)\Version 2001\Version
   2\Standard\Standard\99-7 ver2-0.pdf
       </vers:SourceFileIdentifier>
       <vers:FileRendering>
        <vers:RenderingText>
         <vers:Text>
         See the vers:FileEncoding element
         </vers:Text>
        </vers:RenderingText>
        <vers:RenderingKeywords>
         b64 pdf
        </vers:RenderingKeywords>
       </vers:FileRendering>
      </vers:EncodingMetadata>
      <vers:DocumentData vers:id="Revision:1-Document:1-Encoding:1-
   DocumentData">
JVBERi0xLjMNJeLjz9MNCjEzNyAwIG9iag08PCANL0xpbmVhcml6ZWQgMSANL08gMTM5IA0vSCBb
[...]
ODZiODE+XQ0+Pg1zdGFydHhyZWYNMTczDSUlRU9GDQ==
      </vers:DocumentData>
     </vers:Encoding>
     <vers:Encoding vers:id="Revision:1-Document:1-Encoding:2">
      <vers:EncodingMetadata>
       <vers:FileEncoding>
        <vers:Text>
This encoding is in the native file format for Microsoft Word for Windows 97
Version 8.0 by Microsoft Corporation. The file format has been encoded
into Base64 and the result can be found in the vers:DocumentData tag.
Details of Base64 can be found in the IETF RFC 2045 "Multipurpose Internet
Mail Extensions (MIME) Part One: Format of Internet Message Bodies",
Section 6.8 "Base64 Content-Transfer-Encoding".
        </vers:Text>
       </vers:FileEncoding>
       <vers:SourceFileIdentifier>
        O:\E-RECORD\VERS (97-102)\Standard (99-89)\Version 2001\Version
   2\Standard\Standard\99-7 ver2-0.doc
       </vers:SourceFileIdentifier>
       <vers:FileRendering>
        <vers:RenderingText>
         <vers:Text>
         See the vers:FileEncoding element
         </vers:Text>
        </vers:RenderingText>
        <vers:RenderingKeywords>
         b64 doc
        </vers:RenderingKeywords>
       </vers:FileRendering>
      </vers:EncodingMetadata>
      <vers:DocumentData vers:id="Revision:1-Document:1-Encoding:2-
   DocumentData">
0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAEAAAAiwEAAAAAAAAA
[...]
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
      </vers:DocumentData>
     </vers:Encoding>
    </vers:Document>
    <vers:Document vers:id="Revision:1-Document:2">
     <vers:DocumentMetadata>
```

```
425         <vers:DocumentAgent>
426          <vers:Text>
427           Author: Public Record Office Victoria
428          </vers:Text>
429         </vers:DocumentAgent>
430         <vers:DocumentTitle>
431          <vers:Text>
432           Specification 1: System Requirements for Electronic Records
433          </vers:Text>
434         </vers:DocumentTitle>
435         <vers:DocumentDate>
436          <vers:Text>
437           2003-03-30T05:01:22-10:00
438          </vers:Text>
439         </vers:DocumentDate>
440         <vers:DocumentSource>
441          <vers:Text>
442           Microsoft Word 97 (Version 8)
443          </vers:Text>
444         </vers:DocumentSource>
445        </vers:DocumentMetadata>
446        <vers:Encoding vers:id="Revision:1-Document:2-Encoding:1">
447         <vers:EncodingMetadata>
448          <vers:FileEncoding>
449           <vers:Text>
450  The content of the DocumentData element is a PDF file. The file conforms to
451  'PDF Reference', third edition, Adobe Portable Document Format, Version 1.4,
452  Adobe Systems Incorporated, Addison Wesley, 2001, ISBN 0-201-75839-3
453  (http://partners.adobe.com/asn/developer/acrosdk/docs/filefmtspecs/PDFReference.pdf
454  visited 7 January 2003) as modified in the 'Errata for PDF Reference, third
455  edition' (http://partners.adobe.com/asn/developer/acrosdk/docs/PDF14errata.txt
456  visited 7 January 2003). It may contain digital signatures defined by PDF
457  Public-key Digital Signature and Encryption Specification, Version 3.2, Jim
458  Pravetz, 12 September 2001, Adobe Systems Incorporated
459  (http://partners.adobe.com/asn/developer/pdfs/tn/ppk_pdfspec.pdf visited
460  28 March 2003) and the appearance of the digital signature in a PDF document
461  is defined in Digital Signature Appearances for Public-Key Interoperability,
462  Adobe Systems Incorporated, September 2001
463  (http://partners.adobe.com/asn/developer/pdfs/tn/PPKAppearances.pdf visited
464  28 March 2003). The file has been encoded using Base64 which is defined in
465  IETF RFC 2045 "Multipurpose Internet Mail Extensions (MIME) Part One:
466  Format of Internet Message Bodies", Section 6.8
467  "Base64 Content-Transfer-Encoding".
468           </vers:Text>
469          </vers:FileEncoding>
470          <vers:SourceFileIdentifier>
471           O:\E-RECORD\VERS (97-102)\Standard (99-89)\Version 2001\Version
       2\Standard\Part 1 RKS Functions\99-7-1 Std ver 2-0.pdf
472          </vers:SourceFileIdentifier>
473          <vers:FileRendering>
474           <vers:RenderingText>
475            <vers:Text>
476            See the vers:FileEncoding element
477            </vers:Text>
478           </vers:RenderingText>
479           <vers:RenderingKeywords>
480            b64 pdf
481           </vers:RenderingKeywords>
482          </vers:FileRendering>
483         </vers:EncodingMetadata>
484         <vers:DocumentData vers:id="Revision:1-Document:2-Encoding:1-
       DocumentData">
485  JVBERi0xLjMNJeLjz9MNCjc2IDAgb2JqDTw8IA0vTGluZWFyaXplZCAxIA0vTyA3OCANL0ggWyAz
486  [...]
487  Y2FmMTQzMDM3MGE1ZTlmZj5dDT4+DXN0YXJ0eHJlZg0xNzMNJSVFT0YN
488         </vers:DocumentData>
489        </vers:Encoding>
490       </vers:Document>
491      </vers:Record>
492     </vers:ObjectContent>
493    </vers:SignedObject>
494  </vers:VERSEncapsulatedObject>
```

7.3 Record VEO containing structured documents

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<!DOCTYPE vers:VERSEncapsulatedObject SYSTEM "vers.dtd">
<vers:VERSEncapsulatedObject
  xmlns:vers="http://www.prov.vic.gov.au/gservice/standard/pros99007.htm"
  xmlns:naa="http://www.naa.gov.au/recordkeeping/control/rkms/contents.html">
 <vers:VEOFormatDescription>
  <vers:Text>
This record conforms to the structure defined in "Management of Electronic
Records, PROS 99/007 (Version 2.0)" Public Record Office Victoria, 2003.
The structure of this record is represented using Extensible Markup Language
(XML) 1.0, W3C, 1998
  </vers:Text>
 </vers:VEOFormatDescription>
 <vers:Version>2.0</vers:Version>
 <vers:SignatureBlock vers:id="Revision:1-Signature:1">
  <vers:SignatureFormatDescription>
The contents of this VEO are signed using the SHA-1 hash algorithm and the DSA
digital signature algorithm. SHA-1 is defined in Secure Hash Standard,
FIPS PUB 180-1, National Institute of Standards and Technology, US Department
of Commerce, 17 April 1995
(http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).
The DSA algorithm is defined in Digital Signature Standard (DSS), FIPS PUB
186-2, National Institute of Standards and Technology US Department of
Commerce, 27 January 2000
(http://csrc.nist.gov/publications/fips/fips186-2/fip186-2-change1.pdf).
Details of the public keys are encoded as X.509 certificates in the
vers:CertificateBlock elements. X.509 certificates are defined in "Information
technology - Open Systems Interconnection - The Directory: Public-key and
attribute certificate frameworks", ITU-T Recommendation X.509 (2000).
The signature and certificates are encoded using Base64. Base64 is defined in
Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet
Message Bodies, Section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045,
N. Freed &amp;amp; N. Borenstein, November 1996,
(http://www.ietf.org/rfc/rfc2045.txt?number=2045).
The signature covers the contents of the vers:SignedObject element starting
with the 'less than' symbol of the vers:SignedObject start tag, up to and
including the 'greater than' symbol of the vers:SignedObject end tag. Before
verifying the signature all whitespace (Unicode characters U+0009, U+000A,
U+000D, and U+0020) must be removed from the text.
  </vers:SignatureFormatDescription>
  <vers:SignatureAlgorithm>
   <vers:SignatureAlgorithmIdentifier>
1.2.840.10040.4.3
   </vers:SignatureAlgorithmIdentifier>
  </vers:SignatureAlgorithm>
  <vers:SignatureDate>2003-03-20T11:27:48-10:00</vers:SignatureDate>
  <vers:Signer>PROV Notary (Notary for PROV generated VEOs)</vers:Signer>
  <vers:Signature>
MCwCFChPTcPBV+KkuBb9YZcQEbMbfos7AhQG8yrd91Hz0D5pefIXZutJFwdHbg==
  </vers:Signature>
  <vers:CertificateBlock>
   <vers:Certificate>
MIICoTCCAmGgAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTQxNloXDTAz
MDEyMzAxNDA1NlowMjELMAkGA1UEBhMCQVUxDTALBgNVBAoTBFBST1YxFDASBgNVBAMTC1BST1Yg
Tm90YXJ5MIIBtDCCASkGByqGSM44BAEwggEcAoGA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/
gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfG
G/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFJdgUI8VIwvMspK5
gqLrhAvwWBz1AoGA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCB
gLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhR
kImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAy6h2g/EwZaGzotoIX726y32CzI1rwaNF
reYce1JvOfq94KpVqu79fQl+4tjSyxi0TS/H2RVfcdrKP+8uLTx4CQjzON2uqlvv84Lhg+Dhxc2E
JpH9RlbQa3B0RvILTjeGylcwmVUj+brdT5+foBhQHTIaeHdQsMddzJeB7QVG1cgwCQYHKoZIzjgE
AwMvADAsAhR+T7l7OSF0w9uG65gBeXGzwkMQ9AIUAvB9N2i62E9od7uDZHF1opxP0l4=
   </vers:Certificate>
   <vers:Certificate>
MIICrzCCAm+gAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTIyMVoXDTAz
MDEyMzAxMzkwMVowQDELMAkGA1UEBhMCQVUxIDAeBgNVBAoTF0RvZGd5IEJyb3MgQ2VydGlmaWNh
dGVzMQ8wDQYDVQQDEwZSb290Q0EwggG0MIIBKQYHKoZIzjgEATCCARwCgYD9f1OBHXUSKVLfSpwu
```

```
7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSf
n+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgB
xwIUl2BQjxUjC8yykrmCouuEC/BYHPUCgYD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeC
Z1FZV4661FlP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1
YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYCmx50D/58WrFwa
vjkxGr+Qq9uSQQAzte7gTOlmC1O3P6iYY5zmhZ/uWrXfieZPUK3DGyZfZ3HtG7//U+TgezgYTmyh
uiUIDzWOZlMJCU9CZrKcB5CWfqLY6ijxucMS3NedcbwgOlzVHhfcR+yqLIKh7plogBZYfQttrfSs
wuxJ0TAJBgcqhkjOOAQDAy8AMCwCFD9uWkymtSsiUriiKFEtjfXptP0rAhQ/m2+vVX+W3CpUBiH4
F8cZ5Blhyg==
   </vers:Certificate>
  </vers:CertificateBlock>
 </vers:SignatureBlock>
 <vers:LockSignatureBlock vers:signsSignatureBlock="Revision:1-Signature:1">
  <vers:SignatureFormatDescription>
The contents of this VEO are signed using the SHA-1 hash algorithm and the DSA
digital signature algorithm. SHA-1 is defined in Secure Hash Standard,
FIPS PUB 180-1, National Institute of Standards and Technology, US Department
of Commerce, 17 April 1995
(http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).
The DSA algorithm is defined in Digital Signature Standard (DSS), FIPS PUB
186-2, National Institute of Standards and Technology US Department of
Commerce, 27 January 2000
(http://csrc.nist.gov/publications/fips/fips186-2/fip186-2-change1.pdf).
Details of the public keys are encoded as X.509 certificates in the
vers:CertificateBlock elements. X.509 certificates are defined in "Information
technology - Open Systems Interconnection - The Directory: Public-key and
attribute certificate frameworks", ITU-T Recommendation X.509 (2000).
The signature and certificates are encoded using Base64. Base64 is defined in
Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet
Message Bodies, Section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045,
N. Freed &amp;amp; N. Borenstein, November 1996,
(http://www.ietf.org/rfc/rfc2045.txt?number=2045).
The signature covers the contents of the vers:SignedObject element starting
with the 'less than' symbol of the vers:SignedObject start tag, up to and
including the 'greater than' symbol of the vers:SignedObject end tag. Before
verifying the signature all whitespace (Unicode characters U+0009, U+000A,
U+000D, and U+0020) must be removed from the text.
  </vers:SignatureFormatDescription>
  <vers:SignatureAlgorithm>
   <vers:SignatureAlgorithmIdentifier>
1.2.840.10040.4.3
   </vers:SignatureAlgorithmIdentifier>
  </vers:SignatureAlgorithm>
  <vers:SignatureDate>2003-03-20T11:27:48-10:00</vers:SignatureDate>
  <vers:Signer>PROV Notary (Notary for PROV generated VEOs)</vers:Signer>
  <vers:Signature>
MCwCFChPTcPBV+KkuBb9YZcQEbMbfos7AhQG8yrd91Hz0D5pefIXZutJFwdHbg==
  </vers:Signature>
  <vers:CertificateBlock>
   <vers:Certificate>
MIICoTCCAmGgAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTQxNloXDTAz
MDEyMzAxNDA1NlowMjELMAkGA1UEBhMCQVUxDTALBgNVBAoTBFBST1YxFDASBgNVBAMTC1BST1Yg
Tm90YXJ5MIIBtDCCASkGByqGSM44BAEwggEcAoGA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/
gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfG
G/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFJdgUI8VIwvMspK5
gqLrhAvwWBz1AoGA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCB
gLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhR
kImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAy6h2g/EwZaGzotoIX726y32CzI1rwaNF
reYce1JvOfq94KpVqu79fQl+4tjSyxi0TS/H2RVfcdrKP+8uLTx4CQjzON2uqlvv84Lhg+Dhxc2E
JpH9RlbQa3B0RvILTjeGylcwmVUj+brdT5+foBhQHTIaeHdQsMddzJeB7QVG1cgwCQYHKoZIzjgE
AwMvADAsAhR+T7l7OSF0w9uG65gBeXGzwkMQ9AIUAvB9N2i62E9od7uDZHF1opxP0l4=
   </vers:Certificate>
   <vers:Certificate>
MIICrzCCAm+gAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTIyMVoXDTAz
MDEyMzAxMzkwMVowQDELMAkGA1UEBhMCQVUxIDAeBgNVBAoTF0RvZGd5IEJyb3MgQ2VydGlmaWNh
dGVzMQ8wDQYDVQQDEwZSb290Q0EwggG0MIIBKQYHKoZIzjgEATCCARwCgYD9f1OBHXUSKVLfSpwu
7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSf
n+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgB
xwIUl2BQjxUjC8yykrmCouuEC/BYHPUCgYD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeC
Z1FZV4661FlP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1
YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYCmx50D/58WrFwa
```

```
144  vjkxGr+Qq9uSQQAzte7gTOlmC1O3P6iYY5zmhZ/uWrXfieZPUK3DGyZfZ3HtG7//U+TgezgYTmyh
145  uiUIDzWOZlMJCU9CZrKcB5CWfqLY6ijxucMS3NedcbwgOlzVHhfcR+yqLIKh7plogBZYfQttrfSs
146  wuxJ0TAJBgcqhkjOOAQDAy8AMCwCFD9uWkymtSsiUriiKFEtjfXptP0rAhQ/m2+vVX+W3CpUBiH4
147  F8cZ5Blhyg==
148     </vers:Certificate>
149    </vers:CertificateBlock>
150   </vers:LockSignatureBlock>
151   <vers:SignedObject vers:VEOVersion="2.0">
152    <vers:ObjectMetadata>
153     <vers:ObjectType>Record</vers:ObjectType>
154     <vers:ObjectTypeDescription>
155  This object contains a record; that is a collection of information
156  that must be preserved for a period of time.
157     </vers:ObjectTypeDescription>
158     <vers:ObjectCreationDate>2003-03-20T11:27:40-
       10:00</vers:ObjectCreationDate>
159    </vers:ObjectMetadata>
160    <vers:ObjectContent>
161     <vers:Record>
162      <vers:RecordMetadata>
163       <naa:Agent>
164        <naa:AgentType>
165         Document Author
166        </naa:AgentType>
167        <naa:Jurisdiction>
168         Victoria
169        </naa:Jurisdiction>
170        <naa:CorporateId>
171         VA 683
172        </naa:CorporateId>
173        <naa:CorporateName>
174         Public Record Office Victoria
175        </naa:CorporateName>
176       </naa:Agent>
177       <naa:RightsManagement>
178        <naa:SecurityClassification>
179         Unclassified
180        </naa:SecurityClassification>
181        <naa:UsageCondition>
182         Copyright State of Victoria 2000
183        </naa:UsageCondition>
184       </naa:RightsManagement>
185       <naa:Title>
186        <naa:SchemeType>
187         Free text
188        </naa:SchemeType>
189        <naa:SchemeName>
190         None
191        </naa:SchemeName>
192        <naa:TitleWords>
193         Financial Liability
194        </naa:TitleWords>
195       </naa:Title>
196       <naa:Language>
197        en
198       </naa:Language>
199       <naa:Date>
200        <naa:DateTimeCreated>
201         2003-03-20T23:26:07-10:00
202        </naa:DateTimeCreated>
203        <naa:DateTimeTransacted>
204         2003-03-20T23:26:07-10:00
205        </naa:DateTimeTransacted>
206        <naa:DateTimeRegistered>
207         2003-03-20T23:26:07-10:00
208        </naa:DateTimeRegistered>
209       </naa:Date>
210       <naa:AggregationLevel>
211        Item
212       </naa:AggregationLevel>
213       <naa:ManagementHistory>
214        <vers:ManagementEvent>
215         <naa:EventDateTime>
```

```
216           2003-03-20T23:26:12-10:00
217          </naa:EventDateTime>
218          <naa:EventType>
219           Created
220          </naa:EventType>
221          <naa:EventDescription>
222           Created by user rkm (Rowan McKenzie)
223          </naa:EventDescription>
224         </vers:ManagementEvent>
225         <vers:ManagementEvent>
226          <naa:EventDateTime>
227           2003-03-27T23:26:12-10:00
228          </naa:EventDateTime>
229          <naa:EventType>
230           Custody Transferred
231          </naa:EventType>
232          <naa:EventDescription>
233           Encapsulated in VERS format and exported from Microsoft Exchange to
234           VERS system
235          </naa:EventDescription>
236         </vers:ManagementEvent>
237        </naa:ManagementHistory>
238        <naa:Disposal>
239         <naa:DisposalAuthorisation>
240          No Disposal Coverage
241         </naa:DisposalAuthorisation>
242         <naa:Sentence>
243          No Disposal Coverage
244         </naa:Sentence>
245         <naa:DisposalActionDue>
246          Null
247         </naa:DisposalActionDue>
248         <naa:DisposalStatus>
249          Unknown
250         </naa:DisposalStatus>
251        </naa:Disposal>
252        <vers:VEOIdentifier>
253         <vers:FileIdentifier>
254          <vers:Text>
255           99/876
256          </vers:Text>
257         </vers:FileIdentifier>
258         <vers:VERSRecordIdentifier>
259          <vers:Text>
260           11234
261          </vers:Text>
262         </vers:VERSRecordIdentifier>
263        </vers:VEOIdentifier>
264       </vers:RecordMetadata>
265       <vers:Document
266         vers:id="Revision:1-Document:1"
267         vers:subordinateDocuments="Revision:1-Document:2 Revision:1-Document:5">
268        <vers:DocumentMetadata>
269         <vers:DocumentAgent>
270          <vers:Text>
271           Author: Andrew Waugh
272          </vers:Text>
273         </vers:DocumentAgent>
274         <vers:DocumentTitle>
275          <vers:Text>
276           Email
277          </vers:Text>
278         </vers:DocumentTitle>
279         <vers:DocumentDate>
280          <vers:Text>
281           2003-03-20T23:24:06-10:00
282          </vers:Text>
283         </vers:DocumentDate>
284         <vers:DocumentSource>
285          <vers:Text>
286           Microsoft Word 97
287          </vers:Text>
288         </vers:DocumentSource>
```

```
289       </vers:DocumentMetadata>
290      </vers:Document>
291      <vers:Document
292        vers:id="Revision:1-Document:2"
293        vers:subordinateDocuments="Revision:1-Document:3 Revision:1-Document:4"
294        vers:parentDocument="Revision:1-Document:1">
295       <vers:DocumentMetadata>
296        <vers:DocumentAgent>
297         <vers:Text>
298          Author: Andrew Waugh
299         </vers:Text>
300        </vers:DocumentAgent>
301        <vers:DocumentTitle>
302         <vers:Text>
303          Email Body
304         </vers:Text>
305        </vers:DocumentTitle>
306        <vers:DocumentDate>
307         <vers:Text>
308          2003-03-20T23:24:06-10:00
309         </vers:Text>
310        </vers:DocumentDate>
311        <vers:DocumentSource>
312         <vers:Text>
313          Microsoft Word 97
314         </vers:Text>
315        </vers:DocumentSource>
316       </vers:DocumentMetadata>
317       <vers:Encoding vers:id="Revision:1-Document:2-Encoding:1">
318        <vers:EncodingMetadata>
319         <vers:FileEncoding>
320          <vers:Text>
321  The content of the DocumentData element is a PDF file. The file conforms to
322  'PDF Reference', third edition, Adobe Portable Document Format, Version 1.4,
323  Adobe Systems Incorporated, Addison Wesley, 2001, ISBN 0-201-75839-3
324  (http://partners.adobe.com/asn/developer/acrosdk/docs/filefmtspecs/PDFReferenc
       e.pdf
325  visited 7 January 2003) as modified in the 'Errata for PDF Reference, third
326  edition' (http://partners.adobe.com/asn/developer/acrosdk/docs/PDF14errata.txt
327  visited 7 January 2003). It may contain digital signatures defined by PDF
328  Public-key Digital Signature and Encryption Specification, Version 3.2, Jim
329  Pravetz, 12 September 2001, Adobe Systems Incorporated
330  (http://partners.adobe.com/asn/developer/pdfs/tn/ppk_pdfspec.pdf visited
331  28 March 2003) and the appearance of the digital signature in a PDF document
332  is defined in Digital Signature Appearances for Public-Key Interoperability,
333  Adobe Systems Incorporated, September 2001
334  (http://partners.adobe.com/asn/developer/pdfs/tn/PPKAppearances.pdf visited
335  28 March 2003). The file has been encoded using Base64 which is defined in
336  IETF RFC 2045 "Multipurpose Internet Mail Extensions (MIME) Part One:
337  Format of Internet Message Bodies", Section 6.8
338  "Base64 Content-Transfer-Encoding".
339          </vers:Text>
340         </vers:FileEncoding>
341         <vers:SourceFileIdentifier>
342          P:\Presentations\PublicAccountsCtee\VERSIntegrity.pdf
343         </vers:SourceFileIdentifier>
344         <vers:FileRendering>
345          <vers:RenderingText>
346           <vers:Text>
347            See the vers:FileEncoding element
348           </vers:Text>
349          </vers:RenderingText>
350          <vers:RenderingKeywords>
351           b64 pdf
352          </vers:RenderingKeywords>
353         </vers:FileRendering>
354        </vers:EncodingMetadata>
355        <vers:DocumentData
356          vers:id="Revision:1-Document:2-Encoding:1-DocumentData">
357  JVBERi0xLjMNJeLjz9MNCjkwIDAgb2JqDTw8IA0vTGluZWFyaXplZCAxIA0vTyA5MiANL0ggWyAx
358  [...]
359  MGQ+PDJjNWViMzQ4YjcyNzU3ZGUxODRjMTVjYTVjMjA2YWRhPl0NPj4Nc3RhcnR4cmVmDTE3Mw0l
360  JUVPRg0=
```

```
        </vers:DocumentData>
       </vers:Encoding>
      </vers:Document>
      <vers:Document
        vers:id="Revision:1-Document:3"
        vers:parentDocument="Revision:1-Document:2">
       <vers:DocumentMetadata>
        <vers:DocumentAgent>
         <vers:Text>
          Author: Andrew Waugh
         </vers:Text>
        </vers:DocumentAgent>
        <vers:DocumentTitle>
         <vers:Text>
          Email Attachment 1
         </vers:Text>
        </vers:DocumentTitle>
        <vers:DocumentDate>
         <vers:Text>
          2003-03-20T23:24:06-10:00
         </vers:Text>
        </vers:DocumentDate>
        <vers:DocumentSource>
         <vers:Text>
          Microsoft Word 97
         </vers:Text>
        </vers:DocumentSource>
       </vers:DocumentMetadata>
       <vers:Encoding vers:id="Revision:1-Document:3-Encoding:1">
        <vers:EncodingMetadata>
         <vers:FileEncoding>
          <vers:Text>
The content of the DocumentData element is a PDF file. The file conforms to
‘PDF Reference’, third edition, Adobe Portable Document Format, Version 1.4,
Adobe Systems Incorporated, Addison Wesley, 2001, ISBN 0-201-75839-3
(http://partners.adobe.com/asn/developer/acrosdk/docs/filefmtspecs/PDFReference.pdf
visited 7 January 2003) as modified in the ‘Errata for PDF Reference, third
edition’ (http://partners.adobe.com/asn/developer/acrosdk/docs/PDF14errata.txt
visited 7 January 2003). It may contain digital signatures defined by PDF
Public-key Digital Signature and Encryption Specification, Version 3.2, Jim
Pravetz, 12 September 2001, Adobe Systems Incorporated
(http://partners.adobe.com/asn/developer/pdfs/tn/ppk_pdfspec.pdf visited
28 March 2003) and the appearance of the digital signature in a PDF document
is defined in Digital Signature Appearances for Public-Key Interoperability,
Adobe Systems Incorporated, September 2001
(http://partners.adobe.com/asn/developer/pdfs/tn/PPKAppearances.pdf visited
28 March 2003). The file has been encoded using Base64 which is defined in
IETF RFC 2045 “Multipurpose Internet Mail Extensions (MIME) Part One:
Format of Internet Message Bodies”, Section 6.8
“Base64 Content-Transfer-Encoding”.
          </vers:Text>
         </vers:FileEncoding>
         <vers:SourceFileIdentifier>
          P:\Presentations\PublicAccountsCtee\VERSIntegrity.pdf
         </vers:SourceFileIdentifier>
         <vers:FileRendering>
          <vers:RenderingText>
           <vers:Text>
            See the vers:FileEncoding element
           </vers:Text>
          </vers:RenderingText>
          <vers:RenderingKeywords>
           b64 pdf
          </vers:RenderingKeywords>
         </vers:FileRendering>
        </vers:EncodingMetadata>
        <vers:DocumentData
          vers:id="Revision:1-Document:1-Encoding:3-DocumentData">
JVBERi0xLjMNJeLjz9MNCjkwIDAgb2JqDTw8IA0vTGluZWFyaXplZCAxIA0vTyA5MiANL0ggWyAx
[...]
MGQ+PDJjNWViMzQ4YjcyNzU3ZGUxODRjMTVjYTVjMjA2YWRhPl0NPj4Nc3RhcnR4cmVmDTE3Mw0l
JUVPRg0=
```

```
433         </vers:DocumentData>
434        </vers:Encoding>
435       </vers:Document>
436       <vers:Document
437         vers:id="Revision:1-Document:4"
438         vers:parentDocument="Revision:1-Document:2">
439        <vers:DocumentMetadata>
440         <vers:DocumentAgent>
441          <vers:Text>
442           Author: Andrew Waugh
443          </vers:Text>
444         </vers:DocumentAgent>
445         <vers:DocumentTitle>
446          <vers:Text>
447           Email Attachment 2
448          </vers:Text>
449         </vers:DocumentTitle>
450         <vers:DocumentDate>
451          <vers:Text>
452           2003-03-20T23:24:06-10:00
453          </vers:Text>
454         </vers:DocumentDate>
455         <vers:DocumentSource>
456          <vers:Text>
457           Microsoft Word 97
458          </vers:Text>
459         </vers:DocumentSource>
460        </vers:DocumentMetadata>
461        <vers:Encoding vers:id="Revision:1-Document:4-Encoding:1">
462         <vers:EncodingMetadata>
463          <vers:FileEncoding>
464           <vers:Text>
465  The content of the DocumentData element is a PDF file. The file conforms to
466  'PDF Reference', third edition, Adobe Portable Document Format, Version 1.4,
467  Adobe Systems Incorporated, Addison Wesley, 2001, ISBN 0-201-75839-3
468  (http://partners.adobe.com/asn/developer/acrosdk/docs/filefmtspecs/PDFReferenc
       e.pdf
469  visited 7 January 2003) as modified in the 'Errata for PDF Reference, third
470  edition' (http://partners.adobe.com/asn/developer/acrosdk/docs/PDF14errata.txt
471  visited 7 January 2003). It may contain digital signatures defined by PDF
472  Public-key Digital Signature and Encryption Specification, Version 3.2, Jim
473  Pravetz, 12 September 2001, Adobe Systems Incorporated
474  (http://partners.adobe.com/asn/developer/pdfs/tn/ppk_pdfspec.pdf visited
475  28 March 2003) and the appearance of the digital signature in a PDF document
476  is defined in Digital Signature Appearances for Public-Key Interoperability,
477  Adobe Systems Incorporated, September 2001
478  (http://partners.adobe.com/asn/developer/pdfs/tn/PPKAppearances.pdf visited
479  28 March 2003). The file has been encoded using Base64 which is defined in
480  IETF RFC 2045 "Multipurpose Internet Mail Extensions (MIME) Part One:
481  Format of Internet Message Bodies", Section 6.8
482  "Base64 Content-Transfer-Encoding".
483           </vers:Text>
484          </vers:FileEncoding>
485          <vers:SourceFileIdentifier>
486           P:\Presentations\PublicAccountsCtee\VERSIntegrity.pdf
487          </vers:SourceFileIdentifier>
488          <vers:FileRendering>
489           <vers:RenderingText>
490            <vers:Text>
491             See the vers:FileEncoding element
492            </vers:Text>
493           </vers:RenderingText>
494           <vers:RenderingKeywords>
495            b64 pdf
496           </vers:RenderingKeywords>
497          </vers:FileRendering>
498         </vers:EncodingMetadata>
499         <vers:DocumentData
500           vers:id="Revision:1-Document:4-Encoding:1-DocumentData">
501  JVBERi0xLjMNJeLjz9MNCjkwIDAgb2JqDTw8IA0vTGluZWFyaXplZCAxIA0vTyA5MiANL0ggWyAx
502  [...]
503  MGQ+PDJjNWViMzQ4YjcyNzU3ZGUxODRjMTVjYTVjMjA2YWRhPl0NPj4Nc3RhcnR4cmVmDTE3Mw0l
504  JUVPRg0=
```

```
505         </vers:DocumentData>
506        </vers:Encoding>
507       </vers:Document>
508       <vers:Document
509         vers:id="Revision:1-Document:5"
510         vers:parentDocument="Revision:1-Document:1">
511        <vers:DocumentMetadata>
512         <vers:DocumentAgent>
513          <vers:Text>
514           Author: Andrew Waugh
515          </vers:Text>
516         </vers:DocumentAgent>
517         <vers:DocumentTitle>
518          <vers:Text>
519           Email Headers
520          </vers:Text>
521         </vers:DocumentTitle>
522         <vers:DocumentDate>
523          <vers:Text>
524           2003-03-20T23:24:06-10:00
525          </vers:Text>
526         </vers:DocumentDate>
527         <vers:DocumentSource>
528          <vers:Text>
529           Microsoft Word 97
530          </vers:Text>
531         </vers:DocumentSource>
532        </vers:DocumentMetadata>
533        <vers:Encoding vers:id="Revision:1-Document:5-Encoding:1">
534         <vers:EncodingMetadata>
535          <vers:FileEncoding>
536           <vers:Text>
537  The content of the DocumentData element is a PDF file. The file conforms to
538  'PDF Reference', third edition, Adobe Portable Document Format, Version 1.4,
539  Adobe Systems Incorporated, Addison Wesley, 2001, ISBN 0-201-75839-3
540  (http://partners.adobe.com/asn/developer/acrosdk/docs/filefmtspecs/PDFReferenc
       e.pdf
541  visited 7 January 2003) as modified in the 'Errata for PDF Reference, third
542  edition' (http://partners.adobe.com/asn/developer/acrosdk/docs/PDF14errata.txt
543  visited 7 January 2003). It may contain digital signatures defined by PDF
544  Public-key Digital Signature and Encryption Specification, Version 3.2, Jim
545  Pravetz, 12 September 2001, Adobe Systems Incorporated
546  (http://partners.adobe.com/asn/developer/pdfs/tn/ppk_pdfspec.pdf visited
547  28 March 2003) and the appearance of the digital signature in a PDF document
548  is defined in Digital Signature Appearances for Public-Key Interoperability,
549  Adobe Systems Incorporated, September 2001
550  (http://partners.adobe.com/asn/developer/pdfs/tn/PPKAppearances.pdf visited
551  28 March 2003). The file has been encoded using Base64 which is defined in
552  IETF RFC 2045 "Multipurpose Internet Mail Extensions (MIME) Part One:
553  Format of Internet Message Bodies", Section 6.8
554  "Base64 Content-Transfer-Encoding".
555           </vers:Text>
556          </vers:FileEncoding>
557          <vers:SourceFileIdentifier>
558           P:\Presentations\PublicAccountsCtee\VERSIntegrity.pdf
559          </vers:SourceFileIdentifier>
560          <vers:FileRendering>
561           <vers:RenderingText>
562            <vers:Text>
563             See the vers:FileEncoding element
564            </vers:Text>
565           </vers:RenderingText>
566           <vers:RenderingKeywords>
567            b64 pdf
568           </vers:RenderingKeywords>
569          </vers:FileRendering>
570         </vers:EncodingMetadata>
571         <vers:DocumentData
572           vers:id="Revision:1-Document:1-Encoding:5-DocumentData">
573  JVBERi0xLjMNJeLjz9MNCjkwIDAgb2JqDTw8IA0vTGluZWFyaXplZCAxIA0vTyA5MiANL0ggWyAx
574  [...]
575  MGQ+PDJjNWViMzQ4YjcyNzU3ZGUxODRjMTVjYTVjMjA2YWRhPl0NPj4Nc3RhcnR4cmVmDTE3Mw0l
576  JUVPRg0=
```

```
577         </vers:DocumentData>
578       </vers:Encoding>
579      </vers:Document>
580     </vers:Record>
581    </vers:ObjectContent>
582   </vers:SignedObject>
583  </vers:VERSEncapsulatedObject>
```

7.4 File VEO containing only mandatory and conditional metadata

```
1    <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
2    <!DOCTYPE vers:VERSEncapsulatedObject SYSTEM "vers.dtd">
3    <vers:VERSEncapsulatedObject
4      xmlns:vers="http://www.prov.vic.gov.au/gservice/standard/pros99007.htm"
5      xmlns:naa="http://www.naa.gov.au/recordkeeping/control/rkms/contents.html">
6     <vers:VEOFormatDescription>
7      <vers:Text>
8    This record conforms to the structure defined in "Management of Electronic
9    Records, PROS 99/007 (Version 2.0)" Public Record Office Victoria, 2003
10   The structure of this record is represented using Extensible Markup Language
11   (XML) 1.0, W3C, 1998.
12     </vers:Text>
13    </vers:VEOFormatDescription>
14    <vers:Version>2.0</vers:Version>
15    <vers:SignatureBlock vers:id="Revision:1-Signature:1">
16     <vers:SignatureFormatDescription>
17   The contents of this VEO are signed using the SHA-1 hash algorithm and the DSA
18   digital signature algorithm. SHA-1 is defined in Secure Hash Standard,
19   FIPS PUB 180-1, National Institute of Standards and Technology, US Department
20   of Commerce, 17 April 1995
21   (http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).
22   The DSA algorithm is defined in Digital Signature Standard (DSS), FIPS PUB
23   186-2, National Institute of Standards and Technology US Department of
24   Commerce, 27 January 2000
25   (http://csrc.nist.gov/publications/fips/fips186-2/fip186-2-change1.pdf).
26   Details of the public keys are encoded as X.509 certificates in the
27   vers:CertificateBlock elements. X.509 certificates are defined in "Information
28   technology - Open Systems Interconnection - The Directory: Public-key and
29   attribute certificate frameworks", ITU-T Recommendation X.509 (2000).
30   The signature and certificates are encoded using Base64. Base64 is defined in
31   Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet
32   Message Bodies, Section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045,
33   N. Freed &amp;amp; N. Borenstein, November 1996,
34   (http://www.ietf.org/rfc/rfc2045.txt?number=2045).
35   The signature covers the contents of the vers:SignedObject element starting
36   with the 'less than' symbol of the vers:SignedObject start tag, up to and
37   including the 'greater than' symbol of the vers:SignedObject end tag. Before
38   verifying the signature all whitespace (Unicode characters U+0009, U+000A,
39   U+000D, and U+0020) must be removed from the text.
40     </vers:SignatureFormatDescription>
41     <vers:SignatureAlgorithm>
42      <vers:SignatureAlgorithmIdentifier>
43   1.2.840.10040.4.3
44      </vers:SignatureAlgorithmIdentifier>
45     </vers:SignatureAlgorithm>
46     <vers:SignatureDate>2003-03-30T03:31:17-10:00</vers:SignatureDate>
47     <vers:Signer>PROV Notary (Notary for PROV generated VEOs)</vers:Signer>
48     <vers:Signature>
49   MCwCFE3lX2KCxMJsVNxlV1iqH3gE8WPqAhQX/htenJCyvigBZASUjPDjhuJTJw==
50     </vers:Signature>
51     <vers:CertificateBlock>
52      <vers:Certificate>
53   MIICoTCCAmGgAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
54   eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTQxNloXDTAz
55   MDEyMzAxNDA1NlowMjELMAkGA1UEBhMCQVUxDTALBgNVBAoTBFBST1YxFDASBgNVBAMTC1BST1Yg
56   Tm90YXJ5MIIBtDCCASkGByqGSM44BAEwggEcAoGA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/
57   gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfG
58   G/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFJdgUI8VIwvMspK5
59   gqLrhAvwWBz1AoGA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCB
60   gLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhR
61   kImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAy6h2g/EwZaGzotoIX726y32CzI1rwaNF
```

```
62    reYce1JvOfq94KpVqu79fQl+4tjSyxi0TS/H2RVfcdrKP+8uLTx4CQjzON2uqlvv84Lhg+Dhxc2E
63    JpH9RlbQa3B0RvILTjeGylcwmVUj+brdT5+foBhQHTIaeHdQsMddzJeB7QVG1cgwCQYHKoZIzjgE
64    AwMvADAsAhR+T7l7OSF0w9uG65gBeXGzwkMQ9AIUAvB9N2i62E9od7uDZHF1opxP0l4=
65       </vers:Certificate>
66       <vers:Certificate>
67    MIICrzCCAm+gAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
68    eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTIyMVoXDTAz
69    MDEyMzAxMzkwMVowQDELMAkGA1UEBhMCQVUxIDAeBgNVBAoTF0RvZGd5IEJyb3MgQ2VydGlmaWNh
70    dGVzMQ8wDQYDVQQDEwZSb290Q0EwggG0MIIBKQYHKoZIzjgEATCCARwCgYD9f1OBHXUSKVLfSpwu
71    7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSf
72    n+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgB
73    xwIUl2BQjxUjC8yykrmCouuEC/BYHPUCgYD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeC
74    Z1FZV4661FlP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1
75    YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYCmx50D/58WrFwa
76    vjkxGr+Qq9uSQQAzte7gTOlmC1O3P6iYY5zmhZ/uWrXfieZPUK3DGyZfZ3HtG7//U+TgezgYTmyh
77    uiUIDzWOZlMJCU9CZrKcB5CWfqLY6ijxucMS3NedcbwgOlzVHhfcR+yqLIKh7plogBZYfQttrfSs
78    wuxJ0TAJBgcqhkjOOAQDAy8AMCwCFD9uWkymtSsiUriiKFEtjfXptP0rAhQ/m2+vVX+W3CpUBiH4
79    F8cZ5Blhyg==
80       </vers:Certificate>
81     </vers:CertificateBlock>
82    </vers:SignatureBlock>
83    <vers:LockSignatureBlock vers:signsSignatureBlock="Revision:1-Signature:1">
84     <vers:SignatureFormatDescription>
85    The contents of this VEO is signed using SHA-1 hash algorithm and DSA digital
86    signature algorithm. SHA-1 is defined in Secure Hash Standard, FIPS PUB 180-2,
87    National Institute of Standards and Technology, US Department of Commerce,
88    17 April 1995,
89    (http://csrc.nist.gov/publications/fips/fips180-2/fip180-2.pdf).
90    The DSA algorithm is defined in Digital Signature Standard (DSS), FIPS PUB
91    186-2, National Institute of Standards and Technology US Department of
92    Commerce, 27 January 2000,
93    (http://csrc.nist.gov/publications/fips/fips186-2/fip186-2-change1.pdf).
94    Details of the public keys are encoded as X.509 certificates in the
95    vers:CertificateBlock elements. X.509 certificates are define in "Information
96    technology - Open Systems Interconnection - The Directory: Public-key and
97    attribute certificate frameworks", ITU-T Recommendation X.509 (2000).
98    The signature and certificates are encoded using Base64. Base64 is defined in
99    Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet
100   Message Bodies, Section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045,
101   N. Freed &amp;amp; N. Borenstein, November 1996,
102   (http://www.ietf.org/rfc/rfc2045.txt?number=2045)
103   The signature covers the value of the vers:Signature element contained
104   within the vers:SignatureBlock element identified by the vers:id attribute
105   referenced by the vers:signsSignatureBlock attribute. Before verifying the
106   signature all whitespace (Unicode characters U+0009, U+000A, U+000D, and
107   U+0020) must be removed from the value.
108     </vers:SignatureFormatDescription>
109     <vers:SignatureAlgorithm>
110      <vers:SignatureAlgorithmIdentifier>
111   1.2.840.10040.4.3
112      </vers:SignatureAlgorithmIdentifier>
113     </vers:SignatureAlgorithm>
114     <vers:SignatureDate>2003-03-30T03:31:17-10:00</vers:SignatureDate>
115     <vers:Signer>PROV Notary (Notary for PROV generated VEOs)</vers:Signer>
116     <vers:Signature>
117   MCwCFE3lX2KCxMJsVNxlV1iqH3gE8WPqAhQX/htenJCyvigBZASUjPDjhuJTJw==
118     </vers:Signature>
119     <vers:CertificateBlock>
120      <vers:Certificate>
121   MIICoTCCAmGgAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
122   eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTQxNloXDTAz
123   MDEyMzAxNDA1NlowMjELMAkGA1UEBhMCQVUxDTALBgNVBAoTBFBST1YxFDASBgNVBAMTC1BST1Yg
124   Tm90YXJ5MIIBtDCCASkGByqGSM44BAEwggEcAoGA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/
125   gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfG
126   G/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFJdgUI8VIwvMspK5
127   gqLrhAvwWBz1AoGA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCB
128   gLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhR
129   kImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAy6h2g/EwZaGzotoIX726y32CzI1rwaNF
130   reYce1JvOfq94KpVqu79fQl+4tjSyxi0TS/H2RVfcdrKP+8uLTx4CQjzON2uqlvv84Lhg+Dhxc2E
131   JpH9RlbQa3B0RvILTjeGylcwmVUj+brdT5+foBhQHTIaeHdQsMddzJeB7QVG1cgwCQYHKoZIzjgE
132   AwMvADAsAhR+T7l7OSF0w9uG65gBeXGzwkMQ9AIUAvB9N2i62E9od7uDZHF1opxP0l4=
133      </vers:Certificate>
134      <vers:Certificate>
```

```
MIICrzCCAm+gAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTIyMVoXDTAz
MDEyMzAxMzkwMVowQDELMAkGA1UEBhMCQVUxIDAeBgNVBAoTF0RvZGd5IEJyb3MgQ2VydGlmaWNh
dGVzMQ8wDQYDVQQDEwZSb290Q0EwggG0MIIBKQYHKoZIzjgEATCCARwCgYD9f1OBHXUSKVLfSpwu
7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSf
n+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgB
xwIUl2BQjxUjC8yykrmCouuEC/BYHPUCgYD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeC
Z1FZV4661FlP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1
YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYCmx50D/58WrFwa
vjkxGr+Qq9uSQQAzte7gTOlmC1O3P6iYY5zmhZ/uWrXfieZPUK3DGyZfZ3HtG7//U+TgezgYTmyh
uiUIDzWOZlMJCU9CZrKcB5CWfqLY6ijxucMS3NedcbwgOlzVHhfcR+yqLIKh7plogBZYfQttrfSs
wuxJ0TAJBgcqhkjOOAQDAy8AMCwCFD9uWkymtSsiUriiKFEtjfXptP0rAhQ/m2+vVX+W3CpUBiH4
F8cZ5Blhyg==
   </vers:Certificate>
  </vers:CertificateBlock>
 </vers:LockSignatureBlock>
 <vers:SignedObject vers:VEOVersion="2.0">
  <vers:ObjectMetadata>
   <vers:ObjectType>File</vers:ObjectType>
   <vers:ObjectTypeDescription>
This object contains a file; that is a collection of related records.
   </vers:ObjectTypeDescription>
   <vers:ObjectCreationDate>2003-03-30T03:31:11-
    10:00</vers:ObjectCreationDate>
  </vers:ObjectMetadata>
  <vers:ObjectContent>
   <vers:File>
    <vers:FileMetadata>
     <naa:Agent>
      <naa:AgentType>
       Document Author
      </naa:AgentType>
      <naa:Jurisdiction>
       Victoria
      </naa:Jurisdiction>
      <naa:CorporateName>
       Public Record Office Victoria
      </naa:CorporateName>
     </naa:Agent>
     <naa:RightsManagement>
      <naa:SecurityClassification>
       Unclassified
      </naa:SecurityClassification>
      <naa:UsageCondition>
       Copyright State of Victoria 2000
      </naa:UsageCondition>
     </naa:RightsManagement>
     <naa:Title>
      <naa:SchemeType>
       Free text
      </naa:SchemeType>
      <naa:SchemeName>
       None
      </naa:SchemeName>
      <naa:TitleWords>
       VERS Standard
      </naa:TitleWords>
     </naa:Title>
     <vers:Date>
      <naa:DateTimeCreated>
       2003-03-30T03:28:52-10:00
      </naa:DateTimeCreated>
      <naa:DateTimeTransacted>
       2003-03-30T03:28:52-10:00
      </naa:DateTimeTransacted>
      <naa:DateTimeRegistered>
       2003-03-30T03:28:52-10:00
      </naa:DateTimeRegistered>
     </vers:Date>
     <naa:AggregationLevel>
      File
     </naa:AggregationLevel>
     <naa:ManagementHistory>
```

```
207         <vers:ManagementEvent>
208          <naa:EventDateTime>
209           2003-03-30T03:29:26GMT
210          </naa:EventDateTime>
211          <naa:EventType>
212           Created
213          </naa:EventType>
214          <naa:EventDescription>
215           Created by Clare Green
216          </naa:EventDescription>
217         </vers:ManagementEvent>
218        </naa:ManagementHistory>
219        <naa:Disposal>
220         <naa:DisposalAuthorisation>
221          No Disposal Coverage
222         </naa:DisposalAuthorisation>
223         <naa:Sentence>
224          Permanent
225         </naa:Sentence>
226        </naa:Disposal>
227        <vers:VEOIdentifier>
228         <vers:FileIdentifier>
229          <vers:Text>
230           99-89
231          </vers:Text>
232         </vers:FileIdentifier>
233        </vers:VEOIdentifier>
234       </vers:FileMetadata>
235      </vers:File>
236     </vers:ObjectContent>
237    </vers:SignedObject>
238   </vers:VERSEncapsulatedObject>
```

7.5 File VEO containing optional and conditional metadata

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<!DOCTYPE vers:VERSEncapsulatedObject SYSTEM "vers.dtd">
<vers:VERSEncapsulatedObject
  xmlns:vers="http://www.prov.vic.gov.au/gservice/standard/pros99007.htm"
  xmlns:naa="http://www.naa.gov.au/recordkeeping/control/rkms/contents.html">
 <vers:VEOFormatDescription>
  <vers:Text>
This record conforms to the structure defined in "Management of Electronic
Records, PROS 99/007 (Version 2.0)" Public Record Office Victoria, 2003.
The structure of this record is represented using Extensible Markup Language
(XML) 1.0, W3C, 1998.
  </vers:Text>
 </vers:VEOFormatDescription>
 <vers:Version>2.0</vers:Version>
 <vers:SignatureBlock vers:id="Revision:1-Signature:1">
  <vers:SignatureFormatDescription>
The contents of this VEO are signed using the SHA-1 hash algorithm and the DSA
digital signature algorithm. SHA-1 is defined in Secure Hash Standard,
FIPS PUB 180-1, National Institute of Standards and Technology, US Department
of Commerce, 17 April 1995
(http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).
The DSA algorithm is defined in Digital Signature Standard (DSS), FIPS PUB
186-2, National Institute of Standards and Technology US Department of
Commerce, 27 January 2000
(http://csrc.nist.gov/publications/fips/fips186-2/fip186-2-change1.pdf).
Details of the public keys are encoded as X.509 certificates in the
vers:CertificateBlock elements. X.509 certificates are defined in "Information
technology - Open Systems Interconnection - The Directory: Public-key and
attribute certificate frameworks", ITU-T Recommendation X.509 (2000).
The signature and certificates are encoded using Base64. Base64 is defined in
Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet
Message Bodies, Section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045,
N. Freed &amp;amp; N. Borenstein, November 1996,
(http://www.ietf.org/rfc/rfc2045.txt?number=2045).
The signature covers the contents of the vers:SignedObject element starting
with the 'less than' symbol of the vers:SignedObject start tag, up to and
including the 'greater than' symbol of the vers:SignedObject end tag. Before
verifying the signature all whitespace (Unicode characters U+0009, U+000A,
U+000D, and U+0020) must be removed from the text.
  </vers:SignatureFormatDescription>
  <vers:SignatureAlgorithm>
   <vers:SignatureAlgorithmIdentifier>
1.2.840.10040.4.3
   </vers:SignatureAlgorithmIdentifier>
  </vers:SignatureAlgorithm>
  <vers:SignatureDate>2003-03-30T04:02:29-10:00</vers:SignatureDate>
  <vers:Signer>PROV Notary (Notary for PROV generated VEOs)</vers:Signer>
  <vers:Signature>
MCwCFF3dvbdrGsc0Ypqp4VJsomsSI/MSAhQ/dVgfc/FcwkEGH0edYoJS2fzd9Q==
  </vers:Signature>
  <vers:CertificateBlock>
   <vers:Certificate>
MIICoTCCAmGgAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTQxNloXDTAz
MDEyMzAxNDA1NlowMjELMAkGA1UEBhMCQVUxDTALBgNVBAoTBFBST1YxFDASBgNVBAMTC1BST1Yg
Tm90YXJ5MIIBtDCCASkGByqGSM44BAEwggEcAoGA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/
gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfG
G/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFJdgUI8VIwvMspK5
gqLrhAvwWBz1AoGA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCB
gLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhR
kImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAy6h2g/EwZaGzotoIX726y32CzI1rwaNF
reYce1JvOfq94KpVqu79fQl+4tjSyxi0TS/H2RVfcdrKP+8uLTx4CQjzON2uqlvv84Lhg+Dhxc2E
JpH9RlbQa3B0RvILTjeGylcwmVUj+brdT5+foBhQHTIaeHdQsMddzJeB7QVG1cgwCQYHKoZIzjgE
AwMvADAsAhR+T7l7OSF0w9uG65gBeXGzwkMQ9AIUAvB9N2i62E9od7uDZHF1opxP0l4=
   </vers:Certificate>
   <vers:Certificate>
MIICrzCCAm+gAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTIyMVoXDTAz
```

```
MDEyMzAxMzkwMVowQDELMAkGA1UEBhMCQVUxIDAeBgNVBAoTF0RvZGd5IEJyb3MgQ2VydGlmaWNh
dGVzMQ8wDQYDVQQDEwZSb290Q0EwggG0MIIBKQYHKoZIzjgEATCCARwCgYD9f1OBHXUSKVLfSpwu
7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSf
n+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgB
xwIUl2BQjxUjC8yykrmCouuEC/BYHPUCgYD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeC
Z1FZV4661FlP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1
YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYCmx50D/58WrFwa
vjkxGr+Qq9uSQQAzte7gTOlmC1O3P6iYY5zmhZ/uWrXfieZPUK3DGyZfZ3HtG7//U+TgezgYTmyh
uiUIDzWOZlMJCU9CZrKcB5CWfqLY6ijxucMS3NedcbwgOlzVHhfcR+yqLIKh7plogBZYfQttrfSs
wuxJ0TAJBgcqhkjOOAQDAy8AMCwCFD9uWkymtSsiUriiKFEtjfXptP0rAhQ/m2+vVX+W3CpUBiH4
F8cZ5Blhyg==
      </vers:Certificate>
    </vers:CertificateBlock>
   </vers:SignatureBlock>
   <vers:LockSignatureBlock vers:signsSignatureBlock="Revision:1-Signature:1">
    <vers:SignatureFormatDescription>
The contents of this VEO are signed using the SHA-1 hash algorithm and the DSA
digital signature algorithm. SHA-1 is defined in Secure Hash Standard,
FIPS PUB 180-1, National Institute of Standards and Technology, US Department
of Commerce, 17 April 1995
(http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).
The DSA algorithm is defined in Digital Signature Standard (DSS), FIPS PUB
186-2, National Institute of Standards and Technology US Department of
Commerce, 27 January 2000
(http://csrc.nist.gov/publications/fips/fips186-2/fip186-2-change1.pdf).
Details of the public keys are encoded as X.509 certificates in the
vers:CertificateBlock elements. X.509 certificates are defined in "Information
technology - Open Systems Interconnection - The Directory: Public-key and
attribute certificate frameworks", ITU-T Recommendation X.509 (2000).
The signature and certificates are encoded using Base64. Base64 is defined in
Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet
Message Bodies, Section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045,
N. Freed &amp;amp; N. Borenstein, November 1996,
(http://www.ietf.org/rfc/rfc2045.txt?number=2045).
The signature covers the contents of the vers:SignedObject element starting
with the 'less than' symbol of the vers:SignedObject start tag, up to and
including the 'greater than' symbol of the vers:SignedObject end tag. Before
verifying the signature all whitespace (Unicode characters U+0009, U+000A,
U+000D, and U+0020) must be removed from the text.
    </vers:SignatureFormatDescription>
    <vers:SignatureAlgorithm>
     <vers:SignatureAlgorithmIdentifier>
1.2.840.10040.4.3
     </vers:SignatureAlgorithmIdentifier>
    </vers:SignatureAlgorithm>
    <vers:SignatureDate>2003-03-30T04:02:29-10:00</vers:SignatureDate>
    <vers:Signer>PROV Notary (Notary for PROV generated VEOs)</vers:Signer>
    <vers:Signature>
MCwCFF3dvbdrGsc0Ypqp4VJsomsSI/MSAhQ/dVgfc/FcwkEGH0edYoJS2fzd9Q==
    </vers:Signature>
    <vers:CertificateBlock>
     <vers:Certificate>
MIICoTCCAmGgAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTQxNloXDTAz
MDEyMzAxNDA1NlowMjELMAkGA1UEBhMCQVUxDTALBgNVBAoTBFBST1YxFDASBgNVBAMTC1BST1Yg
Tm90YXJ5MIIBtDCCASkGByqGSM44BAEwggEcAoGA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/
gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfG
G/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFJdgUI8VIwvMspK5
gqLrhAvwWBz1AoGA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCB
gLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhR
kImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAy6h2g/EwZaGzotoIX726y32CzI1rwaNF
reYce1JvOfq94KpVqu79fQl+4tjSyxi0TS/H2RVfcdrKP+8uLTx4CQjzON2uqlvv84Lhg+Dhxc2E
JpH9RlbQa3B0RvILTjeGylcwmVUj+brdT5+foBhQHTIaeHdQsMddzJeB7QVG1cgwCQYHKoZIzjgE
AwMvADAsAhR+T7l7OSF0w9uG65gBeXGzwkMQ9AIUAvB9N2i62E9od7uDZHF1opxP0l4=
     </vers:Certificate>
     <vers:Certificate>
MIICrzCCAm+gAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTIyMVoXDTAz
MDEyMzAxMzkwMVowQDELMAkGA1UEBhMCQVUxIDAeBgNVBAoTF0RvZGd5IEJyb3MgQ2VydGlmaWNh
dGVzMQ8wDQYDVQQDEwZSb290Q0EwggG0MIIBKQYHKoZIzjgEATCCARwCgYD9f1OBHXUSKVLfSpwu
7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSf
n+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgB
xwIUl2BQjxUjC8yykrmCouuEC/BYHPUCgYD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeC
```

```
Z1FZV4661FlP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1
YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYCmx50D/58WrFwa
vjkxGr+Qq9uSQQAzte7gTOlmC1O3P6iYY5zmhZ/uWrXfieZPUK3DGyZfZ3HtG7//U+TgezgYTmyh
uiUIDzWOZlMJCU9CZrKcB5CWfqLY6ijxucMS3NedcbwgOlzVHhfcR+yqLIKh7plogBZYfQttrfSs
wuxJ0TAJBgcqhkjOOAQDAy8AMCwCFD9uWkymtSsiUriiKFEtjfXptP0rAhQ/m2+vVX+W3CpUBiH4
F8cZ5Blhyg==
   </vers:Certificate>
  </vers:CertificateBlock>
 </vers:LockSignatureBlock>
 <vers:SignedObject vers:VEOVersion="2.0">
  <vers:ObjectMetadata>
   <vers:ObjectType>File</vers:ObjectType>
   <vers:ObjectTypeDescription>
This object contains a file; that is a collection of related records
   </vers:ObjectTypeDescription>
   <vers:ObjectCreationDate>2003-03-30T04:02:28-
    10:00</vers:ObjectCreationDate>
  </vers:ObjectMetadata>
  <vers:ObjectContent>
   <vers:File>
    <vers:FileMetadata>
     <naa:Agent>
      <naa:AgentType>
       Document Author
      </naa:AgentType>
      <naa:Jurisdiction>
       Victoria
      </naa:Jurisdiction>
      <naa:CorporateName>
       Public Record Office Victoria
      </naa:CorporateName>
     </naa:Agent>
     <naa:Agent>
      <naa:AgentType>
       Registrar
      </naa:AgentType>
      <naa:Jurisdiction>
       Victoria
      </naa:Jurisdiction>
      <naa:CorporateId>
       VA967
      </naa:CorporateId>
      <naa:CorporateName>
       Department of Infrastructure
      </naa:CorporateName>
      <naa:PersonalName>
       Clare Olive
      </naa:PersonalName>
      <naa:SectionName>
       VERS Centre of Excellence
      </naa:SectionName>
      <naa:PositionName>
       Administrative Assistant
      </naa:PositionName>
      <naa:ContactDetails>
       PO Box 2100 North Melbourne Victoria 3051
      </naa:ContactDetails>
      <naa:Email>
       clare.olive@dpc.vic.gov.au
      </naa:Email>
     </naa:Agent>
     <naa:RightsManagement>
      <naa:SecurityClassification>
       Unclassified
      </naa:SecurityClassification>
      <naa:UsageCondition>
       Copyright State of Victoria 2000
      </naa:UsageCondition>
     </naa:RightsManagement>
     <naa:Title>
      <naa:SchemeType>
       Free text
      </naa:SchemeType>
```

```
214         <naa:SchemeName>
215          None
216         </naa:SchemeName>
217         <naa:TitleWords>
218          VERS Standard
219         </naa:TitleWords>
220        </naa:Title>
221        <vers:Subject>
222         <vers:KeywordLevel>
223          1
224         </vers:KeywordLevel>
225         <vers:Keyword>
226          E-Record
227         </vers:Keyword>
228        </vers:Subject>
229        <vers:Subject>
230         <vers:KeywordLevel>
231          2
232         </vers:KeywordLevel>
233         <vers:Keyword>
234          VERS (96-102)
235         </vers:Keyword>
236        </vers:Subject>
237        <naa:Description>
238  This folder concerns the development and revision of the VERS Standard PROS
       99-007
239        </naa:Description>
240        <naa:Language>
241         en
242        </naa:Language>
243        <naa:Relation>
244         <naa:RelatedItemId>
245          <vers:VEOIdentifier>
246           <vers:FileIdentifier>
247            <vers:Text>
248             99-100
249            </vers:Text>
250           </vers:FileIdentifier>
251          </vers:VEOIdentifier>
252         </naa:RelatedItemId>
253         <naa:RelationType>
254          See also
255         </naa:RelationType>
256         <naa:RelationDescription>
257          See also Stakeholder Liaison (99-100) for surveys
258         </naa:RelationDescription>
259        </naa:Relation>
260        <vers:Date>
261         <naa:DateTimeCreated>
262          2003-03-30T03:28:52-10:00
263         </naa:DateTimeCreated>
264         <naa:DateTimeTransacted>
265          2003-03-30T03:28:52-10:00
266         </naa:DateTimeTransacted>
267         <naa:DateTimeRegistered>
268          2003-03-30T03:28:52-10:00
269         </naa:DateTimeRegistered>
270        </vers:Date>
271        <naa:AggregationLevel>
272         File
273        </naa:AggregationLevel>
274        <naa:ManagementHistory>
275         <vers:ManagementEvent>
276          <naa:EventDateTime>
277           2003-03-30T03:29:26-10:00
278          </naa:EventDateTime>
279          <naa:EventType>
280           Created
281          </naa:EventType>
282          <naa:EventDescription>
283           Created by Clare Green
284          </naa:EventDescription>
285         </vers:ManagementEvent>
```

```
286         <vers:ManagementEvent>
287          <naa:EventDateTime>
288           2003-04-01T11:29:26-10:00
289          </naa:EventDateTime>
290          <naa:EventType>
291           Related
292          </naa:EventType>
293          <naa:EventDescription>
294           Related to Folder 99-100
295          </naa:EventDescription>
296         </vers:ManagementEvent>
297        </naa:ManagementHistory>
298        <naa:Disposal>
299         <naa:DisposalAuthorisation>
300          No Disposal Coverage
301         </naa:DisposalAuthorisation>
302         <naa:Sentence>
303          Permanent
304         </naa:Sentence>
305        </naa:Disposal>
306        <vers:VEOIdentifier>
307         <vers:AgencyIdentifier>
308          <vers:Text>
309           VA 967
310          </vers:Text>
311         </vers:AgencyIdentifier>
312         <vers:SeriesIdentifier>
313          <vers:Text>
314           123
315          </vers:Text>
316         </vers:SeriesIdentifier>
317         <vers:FileIdentifier>
318          <vers:Text>
319           99-89
320          </vers:Text>
321         </vers:FileIdentifier>
322        </vers:VEOIdentifier>
323       </vers:FileMetadata>
324      </vers:File>
325     </vers:ObjectContent>
326    </vers:SignedObject>
327   </vers:VERSEncapsulatedObject>
```

7.6 Modified VEO

Note: The only modifications are:

- The addition of an additional Encoding to the Document.
- The addition of a Management Event refering to the modification.

```
1     <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
2     <!DOCTYPE vers:VERSEncapsulatedObject SYSTEM "vers.dtd">
3     <vers:VERSEncapsulatedObject
4       xmlns:vers="http://www.prov.vic.gov.au/gservice/standard/pros99007.htm"
5       xmlns:naa="http://www.naa.gov.au/recordkeeping/control/rkms/contents.html">
6      <vers:VEOFormatDescription>
7       <vers:Text>
8     This record conforms to the structure defined in "Management of Electronic
9     Records, PROS 99/007 (Version 2.0)" Public Record Office Victoria, 2003.
10    The structure of this record is represented using Extensible Markup Language
11    (XML) 1.0, W3C, 1998
12      </vers:Text>
13     </vers:VEOFormatDescription>
14     <vers:Version>2.0</vers:Version>
15     <vers:SignatureBlock vers:id="Revision:2-Signature:1">
16      <vers:SignatureFormatDescription>
17    The contents of this VEO are signed using the SHA-1 hash algorithm and the DSA
18    digital signature algorithm. SHA-1 is defined in Secure Hash Standard,
```

```
FIPS PUB 180-1, National Institute of Standards and Technology, US Department
of Commerce, 17 April 1995
(http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).
The DSA algorithm is defined in Digital Signature Standard (DSS), FIPS PUB
186-2, National Institute of Standards and Technology US Department of
Commerce, 27 January 2000
(http://csrc.nist.gov/publications/fips/fips186-2/fip186-2-change1.pdf).
Details of the public keys are encoded as X.509 certificates in the
vers:CertificateBlock elements. X.509 certificates are defined in "Information
technology - Open Systems Interconnection - The Directory: Public-key and
attribute certificate frameworks", ITU-T Recommendation X.509 (2000).
The signature and certificates are encoded using Base64. Base64 is defined in
Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet
Message Bodies, Section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045,
N. Freed &amp;amp; N. Borenstein, November 1996,
(http://www.ietf.org/rfc/rfc2045.txt?number=2045).
The signature covers the contents of the vers:SignedObject element starting
with the 'less than' symbol of the vers:SignedObject start tag, up to and
including the 'greater than' symbol of the vers:SignedObject end tag. Before
verifying the signature all whitespace (Unicode characters U+0009, U+000A,
U+000D, and U+0020) must be removed from the text.
  </vers:SignatureFormatDescription>
  <vers:SignatureAlgorithm>
   <vers:SignatureAlgorithmIdentifier>
1.2.840.10040.4.3
   </vers:SignatureAlgorithmIdentifier>
  </vers:SignatureAlgorithm>
  <vers:SignatureDate>2003-03-20T11:27:48-10:00</vers:SignatureDate>
  <vers:Signer>PROV Notary (Notary for PROV generated VEOs)</vers:Signer>
  <vers:Signature>
MCwCFChPTcPBV+KkuBb9YZcQEbMbfos7AhQG8yrd91Hz0D5pefIXZutJFwdHbg==
  </vers:Signature>
  <vers:CertificateBlock>
   <vers:Certificate>
MIICoTCCAmGgAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTQxNloXDTAz
MDEyMzAxNDA1NlowMjELMAkGA1UEBhMCQVUxDTALBgNVBAoTBFBST1YxFDASBgNVBAMTC1BST1Yg
Tm90YXJ5MIIBtDCCASkGByqGSM44BAEwggEcAoGA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/
gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfG
G/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFJdgUI8VIwvMspK5
gqLrhAvwWBz1AoGA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCB
gLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhR
kImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAy6h2g/EwZaGzotoIX726y32CzI1rwaNF
reYce1JvOfq94KpVqu79fQl+4tjSyxi0TS/H2RVfcdrKP+8uLTx4CQjzON2uqlvv84Lhg+Dhxc2E
JpH9RlbQa3B0RvILTjeGylcwmVUj+brdT5+foBhQHTIaeHdQsMddzJeB7QVG1cgwCQYHKoZIzjgE
AwMvADAsAhR+T7l7OSF0w9uG65gBeXGzwkMQ9AIUAvB9N2i62E9od7uDZHF1opxP0l4=
   </vers:Certificate>
   <vers:Certificate>
MIICrzCCAm+gAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTIyMVoXDTAz
MDEyMzAxMzkwMVowQDELMAkGA1UEBhMCQVUxIDAeBgNVBAoTF0RvZGd5IEJyb3MgQ2VydGlmaWNh
dGVzMQ8wDQYDVQQDEwZSb290Q0EwggG0MIIBKQYHKoZIzjgEATCCARwCgYD9f1OBHXUSKVLfSpwu
7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSf
n+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgB
xwIUl2BQjxUjC8yykrmCouuEC/BYHPUCgYD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeC
Z1FZV4661FlP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1
YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYCmx50D/58WrFwa
vjkxGr+Qq9uSQQAzte7gTOlmC1O3P6iYY5zmhZ/uWrXfieZPUK3DGyZfZ3HtG7//U+TgezgYTmyh
uiUIDzWOZlMJCU9CZrKcB5CWfqLY6ijxucMS3NedcbwgOlzVHhfcR+yqLIKh7plogBZYfQttrfSs
wuxJ0TAJBgcqhkjOOAQDAy8AMCwCFD9uWkymtSsiUriiKFEtjfXptP0rAhQ/m2+vVX+W3CpUBiH4
F8cZ5Blhyg==
   </vers:Certificate>
  </vers:CertificateBlock>
 </vers:SignatureBlock>
 <vers:LockSignatureBlock vers:signsSignatureBlock="Revision:2-Signature:1">
  <vers:SignatureFormatDescription>
The contents of this VEO are signed using the SHA-1 hash algorithm and the DSA
digital signature algorithm. SHA-1 is defined in Secure Hash Standard,
FIPS PUB 180-1, National Institute of Standards and Technology, US Department
of Commerce, 17 April 1995
(http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).
The DSA algorithm is defined in Digital Signature Standard (DSS), FIPS PUB
186-2, National Institute of Standards and Technology US Department of
```

```
92   Commerce, 27 January 2000
93   (http://csrc.nist.gov/publications/fips/fips186-2/fip186-2-change1.pdf).
94   Details of the public keys are encoded as X.509 certificates in the
95   vers:CertificateBlock elements. X.509 certificates are defined in "Information
96   technology - Open Systems Interconnection - The Directory: Public-key and
97   attribute certificate frameworks", ITU-T Recommendation X.509 (2000).
98   The signature and certificates are encoded using Base64. Base64 is defined in
99   Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet
100  Message Bodies, Section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045,
101  N. Freed &amp;amp; N. Borenstein, November 1996,
102  (http://www.ietf.org/rfc/rfc2045.txt?number=2045).
103  The signature covers the contents of the vers:SignedObject element starting
104  with the 'less than' symbol of the vers:SignedObject start tag, up to and
105  including the 'greater than' symbol of the vers:SignedObject end tag. Before
106  verifying the signature all whitespace (Unicode characters U+0009, U+000A,
107  U+000D, and U+0020) must be removed from the text.
108    </vers:SignatureFormatDescription>
109    <vers:SignatureAlgorithm>
110     <vers:SignatureAlgorithmIdentifier>
111  1.2.840.10040.4.3
112     </vers:SignatureAlgorithmIdentifier>
113    </vers:SignatureAlgorithm>
114    <vers:SignatureDate>2003-03-20T11:27:48-10:00</vers:SignatureDate>
115    <vers:Signer>PROV Notary (Notary for PROV generated VEOs)</vers:Signer>
116    <vers:Signature>
117  MCwCFChPTcPBV+KkuBb9YZcQEbMbfos7AhQG8yrd91Hz0D5pefIXZutJFwdHbg==
118    </vers:Signature>
119    <vers:CertificateBlock>
120     <vers:Certificate>
121  MIICoTCCAmGgAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
122  eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTQxNloXDTAz
123  MDEyMzAxNDA1NlowMjELMAkGA1UEBhMCQVUxDTALBgNVBAoTBFBST1YxFDASBgNVBAMTC1BST1Yg
124  Tm90YXJ5MIIBtDCCASkGByqGSM44BAEwggEcAoGA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/
125  gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfG
126  G/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFJdgUI8VIwvMspK5
127  gqLrhAvwWBz1AoGA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCB
128  gLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhR
129  kImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAy6h2g/EwZaGzotoIX726y32CzI1rwaNF
130  reYce1JvOfq94KpVqu79fQl+4tjSyxi0TS/H2RVfcdrKP+8uLTx4CQjzON2uqlvv84Lhg+Dhxc2E
131  JpH9RlbQa3B0RvILTjeGylcwmVUj+brdT5+foBhQHTIaeHdQsMddzJeB7QVG1cgwCQYHKoZIzjgE
132  AwMvADAsAhR+T7l7OSF0w9uG65gBeXGzwkMQ9AIUAvB9N2i62E9od7uDZHF1opxP0l4=
133     </vers:Certificate>
134     <vers:Certificate>
135  MIICrzCCAm+gAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
136  eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTIyMVoXDTAz
137  MDEyMzAxMzkwMVowQDELMAkGA1UEBhMCQVUxIDAeBgNVBAoTF0RvZGd5IEJyb3MgQ2VydGlmaWNh
138  dGVzMQ8wDQYDVQQDEwZSb290Q0EwggG0MIIBKQYHKoZIzjgEATCCARwCgYD9f1OBHXUSKVLfSpwu
139  7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSf
140  n+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgB
141  xwIUl2BQjxUjC8yykrmCouuEC/BYHPUCgYD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeC
142  Z1FZV4661FlP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1
143  YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYCmx50D/58WrFwa
144  vjkxGr+Qq9uSQQAzte7gTOlmC1O3P6iYY5zmhZ/uWrXfieZPUK3DGyZfZ3HtG7//U+TgezgYTmyh
145  uiUIDzWOZlMJCU9CZrKcB5CWfqLY6ijxucMS3NedcbwgOlzVHhfcR+yqLIKh7plogBZYfQttrfSs
146  wuxJ0TAJBgcqhkjOOAQDAy8AMCwCFD9uWkymtSsiUriiKFEtjfXptP0rAhQ/m2+vVX+W3CpUBiH4
147  F8cZ5Blhyg==
148     </vers:Certificate>
149    </vers:CertificateBlock>
150   </vers:LockSignatureBlock>
151   <vers:SignedObject vers:VEOVersion="2.0">
152    <vers:ObjectMetadata>
153     <vers:ObjectType>Modified VEO</vers:ObjectType>
154     <vers:ObjectTypeDescription>
155  This object contains a VEO which has been modified. The Modified VEO may
156  be a record VEO, a file VEO, or another Modified VEO.
157     </vers:ObjectTypeDescription>
158     <vers:ObjectCreationDate>2003-03-20T11:27:40-
       10:00</vers:ObjectCreationDate>
159    </vers:ObjectMetadata>
160    <vers:ObjectContent>
161     <vers:ModifiedVEO vers:OriginalVEOType=”Record”>
162      <vers:DateTimeModified>
163       2003-03-31T15:26:07-10:00
```

```
164       </vers:DateTimeModified>
165       <vers:RevisedVEO vers:id=”Revision:2”>
166    <vers:SignedObject vers:VEOVersion="2.0">
167     <vers:ObjectMetadata>
168      <vers:ObjectType>Record</vers:ObjectType>
169      <vers:ObjectTypeDescription>
170  This object contains a record; that is a collection of information
171  that must be preserved for a period of time.
172     </vers:ObjectTypeDescription>
173     <vers:ObjectCreationDate>2003-03-30T05:04:10-
        10:00</vers:ObjectCreationDate>
174    </vers:ObjectMetadata>
175    <vers:ObjectContent>
176     <vers:Record>
177      <vers:RecordMetadata>
178       <naa:Agent>
179        <naa:AgentType>
180         Document Author
181        </naa:AgentType>
182        <naa:Jurisdiction>
183         Victoria
184        </naa:Jurisdiction>
185        <naa:CorporateId>
186         VA 683
187        </naa:CorporateId>
188        <naa:CorporateName>
189         Public Record Office Victoria
190        </naa:CorporateName>
191       </naa:Agent>
192       <naa:RightsManagement>
193        <naa:SecurityClassification>
194         Unclassified
195        </naa:SecurityClassification>
196        <naa:UsageCondition>
197         Copyright State of Victoria 2000
198        </naa:UsageCondition>
199       </naa:RightsManagement>
200       <naa:Title>
201        <naa:SchemeType>
202         Free text
203        </naa:SchemeType>
204        <naa:SchemeName>
205         None
206        </naa:SchemeName>
207        <naa:TitleWords>
208         Integrity of Government Information, The VERS Experience
209        </naa:TitleWords>
210       </naa:Title>
211       <naa:Language>
212        en
213       </naa:Language>
214       <naa:Date>
215        <naa:DateTimeCreated>
216         2003-03-20T23:26:07-10:00
217        </naa:DateTimeCreated>
218        <naa:DateTimeTransacted>
219         2003-03-20T23:26:07-10:00
220        </naa:DateTimeTransacted>
221        <naa:DateTimeRegistered>
222         2003-03-20T23:26:07-10:00
223        </naa:DateTimeRegistered>
224       </naa:Date>
225       <naa:AggregationLevel>
226        Item
227       </naa:AggregationLevel>
228       <naa:ManagementHistory>
229        <vers:ManagementEvent>
230         <naa:EventDateTime>
231          2003-03-20T23:26:12-10:00
232         </naa:EventDateTime>
233         <naa:EventType>
234          Created
235         </naa:EventType>
```

```
236          <naa:EventDescription>
237           Created by user rkm (Rowan McKenzie)
238          </naa:EventDescription>
239         </vers:ManagementEvent>
240         <vers:ManagementEvent>
241          <naa:EventDateTime>
242           2003-03-27T23:26:12-10:00
243          </naa:EventDateTime>
244          <naa:EventType>
245           Custody Transferred
246          </naa:EventType>
247          <naa:EventDescription>
248           Encapsulated in VERS format and exported from EMPS system to
249           VERS system
250          </naa:EventDescription>
251         </vers:ManagementEvent>
252         <vers:ManagementEvent>
253          <naa:EventDateTime>
254           2003-03-31T15:26:07-10:00
255          </naa:EventDateTime>
256          <naa:EventType>
257           Modified
258          </naa:EventType>
259          <naa:EventDescription>
260           Record modified and Modified VEO created by John Smith. All digital
261           signatures on the original VEO were successfully validated.
262          </naa:EventDescription>
263         </vers:ManagementEvent>
264        </naa:ManagementHistory>
265        <naa:Disposal>
266         <naa:DisposalAuthorisation>
267          No Disposal Coverage
268         </naa:DisposalAuthorisation>
269         <naa:Sentence>
270          No Disposal Coverage
271         </naa:Sentence>
272         <naa:DisposalActionDue>
273          Null
274         </naa:DisposalActionDue>
275         <naa:DisposalStatus>
276          Unknown
277         </naa:DisposalStatus>
278        </naa:Disposal>
279        <vers:VEOIdentifier>
280         <vers:FileIdentifier>
281          <vers:Text>
282           99/876
283          </vers:Text>
284         </vers:FileIdentifier>
285         <vers:VERSRecordIdentifier>
286          <vers:Text>
287           11234
288          </vers:Text>
289         </vers:VERSRecordIdentifier>
290        </vers:VEOIdentifier>
291       </vers:RecordMetadata>
292       <vers:Document vers:id="Revision:2-Document:1">
293        <vers:DocumentMetadata>
294         <vers:DocumentAgent>
295          <vers:Text>
296           Author: Andrew Waugh
297          </vers:Text>
298         </vers:DocumentAgent>
299         <vers:DocumentTitle>
300          <vers:Text>
301           Report
302          </vers:Text>
303         </vers:DocumentTitle>
304         <vers:DocumentDate>
305          <vers:Text>
306           2003-03-20T23:24:06-10:00
307          </vers:Text>
308         </vers:DocumentDate>
```

```
      <vers:DocumentSource>
       <vers:Text>
        Microsoft Word 97
       </vers:Text>
      </vers:DocumentSource>
     </vers:DocumentMetadata>
     <vers:Encoding vers:id="Revision:2-Document:1-Encoding:1">
      <vers:EncodingMetadata>
       <vers:FileEncoding>
        <vers:Text>
This encoding is in the native file format for Microsoft Word for Windows 97
Version 8.0 by Microsoft Corporation. The file format has been encoded
into Base64 and the result can be found in the vers:DocumentData tag.
Details of Base64 can be found in the IETF RFC 2045 "Multipurpose Internet
Mail Extensions (MIME) Part One: Format of Internet Message Bodies",
Section 6.8 "Base64 Content-Transfer-Encoding".
        </vers:Text>
       </vers:FileEncoding>
       <vers:SourceFileIdentifier>
        P:\Presentations\PublicAccountsCtee\VERSIntegrity.doc
       </vers:SourceFileIdentifier>
       <vers:FileRendering>
        <vers:RenderingText>
         <vers:Text>
         See the vers:FileEncoding element
         </vers:Text>
        </vers:RenderingText>
        <vers:RenderingKeywords>
         b64 doc
        </vers:RenderingKeywords>
       </vers:FileRendering>
      </vers:EncodingMetadata>
      <vers:DocumentData vers:id="Revision:2-Document:1-Encoding:1-DocumentData">
0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAAAEAAAAiwEAAAAAAAAA
[...]
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
      </vers:DocumentData>
     </vers:Encoding>
     <vers:Encoding vers:id="Revision:2-Document:1-Encoding:2">
      <vers:EncodingMetadata>
       <vers:FileEncoding>
        <vers:Text>
The content of the DocumentData element is a PDF file. The file conforms to
'PDF Reference', third edition, Adobe Portable Document Format, Version 1.4,
Adobe Systems Incorporated, Addison Wesley, 2001, ISBN 0-201-75839-3
(http://partners.adobe.com/asn/developer/acrosdk/docs/filefmtspecs/PDFReference.pdf
visited 7 January 2003) as modified in the 'Errata for PDF Reference, third
edition' (http://partners.adobe.com/asn/developer/acrosdk/docs/PDF14errata.txt
visited 7 January 2003). It may contain digital signatures defined by PDF
Public-key Digital Signature and Encryption Specification, Version 3.2, Jim
Pravetz, 12 September 2001, Adobe Systems Incorporated
(http://partners.adobe.com/asn/developer/pdfs/tn/ppk_pdfspec.pdf visited
28 March 2003) and the appearance of the digital signature in a PDF document
is defined in Digital Signature Appearances for Public-Key Interoperability,
Adobe Systems Incorporated, September 2001
(http://partners.adobe.com/asn/developer/pdfs/tn/PPKAppearances.pdf visited
28 March 2003). The file has been encoded using Base64 which is defined in
IETF RFC 2045 "Multipurpose Internet Mail Extensions (MIME) Part One:
Format of Internet Message Bodies", Section 6.8
"Base64 Content-Transfer-Encoding".
        </vers:Text>
       </vers:FileEncoding>
       <vers:SourceFileIdentifier>
        P:\Presentations\PublicAccountsCtee\VERSIntegrity.pdf
       </vers:SourceFileIdentifier>
       <vers:FileRendering>
        <vers:RenderingText>
         <vers:Text>
          See the vers:FileEncoding element
         </vers:Text>
        </vers:RenderingText>
```

```
380           <vers:RenderingKeywords>
381            b64 pdf
382           </vers:RenderingKeywords>
383         </vers:FileRendering>
384        </vers:EncodingMetadata>
385        <vers:DocumentData
386          vers:id="Revision:2-Document:1-Encoding:2-DocumentData"
387          vers:forContentsSeeElement="Revision:1-Document:1-Encoding:1"/>
388       </vers:Encoding>
389      </vers:Document>
390     </vers:Record>
391    </vers:ObjectContent>
392   </vers:SignedObject>
393      </vers:RevisedVEO>
394      <vers:OriginalVEO>
395       <vers:Version>2.0</vers:Version>
396   <vers:SignatureBlock vers:id="Revision:1-Signature:1">
397    <vers:SignatureFormatDescription>
398  The contents of this VEO are signed using the SHA-1 hash algorithm and the DSA
399  digital signature algorithm. SHA-1 is defined in Secure Hash Standard,
400  FIPS PUB 180-1, National Institute of Standards and Technology, US Department
401  of Commerce, 17 April 1995
402  (http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).
403  The DSA algorithm is defined in Digital Signature Standard (DSS), FIPS PUB
404  186-2, National Institute of Standards and Technology US Department of
405  Commerce, 27 January 2000
406  (http://csrc.nist.gov/publications/fips/fips186-2/fip186-2-change1.pdf).
407  Details of the public keys are encoded as X.509 certificates in the
408  vers:CertificateBlock elements. X.509 certificates are defined in "Information
409  technology - Open Systems Interconnection - The Directory: Public-key and
410  attribute certificate frameworks", ITU-T Recommendation X.509 (2000).
411  The signature and certificates are encoded using Base64. Base64 is defined in
412  Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet
413  Message Bodies, Section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045,
414  N. Freed &amp;amp; N. Borenstein, November 1996,
415  (http://www.ietf.org/rfc/rfc2045.txt?number=2045).
416  The signature covers the contents of the vers:SignedObject element starting
417  with the 'less than' symbol of the vers:SignedObject start tag, up to and
418  including the 'greater than' symbol of the vers:SignedObject end tag. Before
419  verifying the signature all whitespace (Unicode characters U+0009, U+000A,
420  U+000D, and U+0020) must be removed from the text.
421    </vers:SignatureFormatDescription>
422    <vers:SignatureAlgorithm>
423     <vers:SignatureAlgorithmIdentifier>
424  1.2.840.10040.4.3
425     </vers:SignatureAlgorithmIdentifier>
426    </vers:SignatureAlgorithm>
427    <vers:SignatureDate>2003-03-30T05:04:25-10:00</vers:SignatureDate>
428    <vers:Signer>PROV Notary (Notary for PROV generated VEOs)</vers:Signer>
429    <vers:Signature>
430  MCwCFDEkcxNAD23bVijId7BddMqDbograhQS336tarMu3kec3gpfGQa4uc+m6g==
431    </vers:Signature>
432    <vers:CertificateBlock>
433     <vers:Certificate>
434  MIICoTCCAmGgAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
435  eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTQxNloXDTAz
436  MDEyMzAxNDA1NlowMjELMAkGA1UEBhMCQVUxDTALBgNVBAoTBFBST1YxFDASBgNVBAMTC1BST1Yg
437  Tm90YXJ5MIIBtDCCASkGByqGSM44BAEwggEcAoGA/X9TgR11EilS30qcLuzk5/YRt1I870QAwx4/
438  gLZRJmlFXUAiUftZPY1Y+r/F9bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu6nX/rfG
439  G/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2dfOuK2HXKu/yIgMZndFIAccCFJdgUI8VIwvMspK5
440  gqLrhAvwWBz1AoGA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCB
441  gLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhR
442  kImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAy6h2g/EwZaGzotoIX726y32CzI1rwaNF
443  reYce1JvOfq94KpVqu79fQl+4tjSyxi0TS/H2RVfcdrKP+8uLTx4CQjzON2uqlvv84Lhg+Dhxc2E
444  JpH9RlbQa3B0RvILTjeGylcwmVUj+brdT5+foBhQHTIaeHdQsMddzJeB7QVG1cgwCQYHKoZIzjgE
445  AwMvADAsAhR+T7l7OSF0w9uG65gBeXGzwkMQ9AIUAvB9N2i62E9od7uDZHF1opxP0l4=
446     </vers:Certificate>
447     <vers:Certificate>
448  MIICrzCCAm+gAwIBAgIBETAJBgcqhkjOOAQDMEAxCzAJBgNVBAYTAkFVMSAwHgYDVQQKExdEb2Rn
449  eSBCcm9zIENlcnRpZmljYXRlczEPMA0GA1UEAxMGUm9vdENBMB4XDTAzMDEyMjEwNTIyMVoXDTAz
450  MDEyMzAxMzkwMVowQDELMAkGA1UEBhMCQVUxIDAeBgNVBAoTF0RvZGd5IEJyb3MgQ2VydGlmaWNh
451  dGVzMQ8wDQYDVQQDEwZSb290Q0EwggG0MIIBKQYHKoZIzjgEATCCARwCgYD9f1OBHXUSKVLfSpwu
452  7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2y5tVbNeBO4AdNG/yZmC3a5lQpaSf
```

```
n+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQTWhaRMvZ1864rYdcq7/IiAxmd0UgB
xwIUl2BQjxUjC8yykrmCouuEC/BYHPUCgYD34aCF1ps93su8q1w2uFe5eZSvu/o66oL5V0wLPQeC
Z1FZV4661FlP5nEHEIGAtEkWcSPoTCgWE7fPCTKMyKbhPBZ6i1R8jSjgo64eK7OmdZFuo38L+iE1
YvH7YnoBJDvMpPG+qFGQiaiD3+Fa5Z8GkotmXoB7VSVkAUw7/s9JKgOBhAACgYCmx50D/58WrFwa
vjkxGr+Qq9uSQQAzte7gTOlmC1O3P6iYY5zmhZ/uWrXfieZPUK3DGyZfZ3HtG7//U+TgezgYTmyh
uiUIDzWOZlMJCU9CZrKcB5CWfqLY6ijxucMS3NedcbwgOlzVHhfcR+yqLIKh7plogBZYfQttrfSs
wuxJ0TAJBgcqhkjOOAQDAy8AMCwCFD9uWkymtSsiUriiKFEtjfXptP0rAhQ/m2+vVX+W3CpUBiH4
F8cZ5Blhyg==
   </vers:Certificate>
  </vers:CertificateBlock>
 </vers:SignatureBlock>
 <vers:SignedObject vers:VEOVersion="2.0">
  <vers:ObjectMetadata>
   <vers:ObjectType>Record</vers:ObjectType>
   <vers:ObjectTypeDescription>
This object contains a record; that is a collection of information
that must be preserved for a period of time.
   </vers:ObjectTypeDescription>
   <vers:ObjectCreationDate>2003-03-30T05:04:10-
   10:00</vers:ObjectCreationDate>
  </vers:ObjectMetadata>
  <vers:ObjectContent>
   <vers:Record>
    <vers:RecordMetadata>
     <naa:Agent>
      <naa:AgentType>
       Document Author
      </naa:AgentType>
      <naa:Jurisdiction>
       Victoria
      </naa:Jurisdiction>
      <naa:CorporateId>
       VA 683
      </naa:CorporateId>
      <naa:CorporateName>
       Public Record Office Victoria
      </naa:CorporateName>
     </naa:Agent>
     <naa:RightsManagement>
      <naa:SecurityClassification>
       Unclassified
      </naa:SecurityClassification>
      <naa:UsageCondition>
       Copyright State of Victoria 2000
      </naa:UsageCondition>
     </naa:RightsManagement>
     <naa:Title>
      <naa:SchemeType>
       Free text
      </naa:SchemeType>
      <naa:SchemeName>
       None
      </naa:SchemeName>
      <naa:TitleWords>
       Integrity of Government Information, The VERS Experience
      </naa:TitleWords>
     </naa:Title>
     <naa:Language>
      en
     </naa:Language>
     <naa:Date>
      <naa:DateTimeCreated>
       2003-03-20T23:26:07-10:00
      </naa:DateTimeCreated>
      <naa:DateTimeTransacted>
       2003-03-20T23:26:07-10:00
      </naa:DateTimeTransacted>
      <naa:DateTimeRegistered>
       2003-03-20T23:26:07-10:00
      </naa:DateTimeRegistered>
     </naa:Date>
     <naa:AggregationLevel>
      Item
```

```
525       </naa:AggregationLevel>
526       <naa:ManagementHistory>
527        <vers:ManagementEvent>
528         <naa:EventDateTime>
529          2003-03-20T23:26:12-10:00
530         </naa:EventDateTime>
531         <naa:EventType>
532          Created
533         </naa:EventType>
534         <naa:EventDescription>
535          Created by user rkm (Rowan McKenzie)
536         </naa:EventDescription>
537        </vers:ManagementEvent>
538        <vers:ManagementEvent>
539         <naa:EventDateTime>
540          2003-03-27T23:26:12-10:00
541         </naa:EventDateTime>
542         <naa:EventType>
543          Custody Transferred
544         </naa:EventType>
545         <naa:EventDescription>
546          Encapsulated in VERS format and exported from EMPS system to
547          VERS system
548         </naa:EventDescription>
549        </vers:ManagementEvent>
550       </naa:ManagementHistory>
551       <naa:Disposal>
552        <naa:DisposalAuthorisation>
553         No Disposal Coverage
554        </naa:DisposalAuthorisation>
555        <naa:Sentence>
556         No Disposal Coverage
557        </naa:Sentence>
558        <naa:DisposalActionDue>
559         Null
560        </naa:DisposalActionDue>
561        <naa:DisposalStatus>
562         Unknown
563        </naa:DisposalStatus>
564       </naa:Disposal>
565       <vers:VEOIdentifier>
566        <vers:FileIdentifier>
567         <vers:Text>
568          99/876
569         </vers:Text>
570        </vers:FileIdentifier>
571        <vers:VERSRecordIdentifier>
572         <vers:Text>
573          11234
574         </vers:Text>
575        </vers:VERSRecordIdentifier>
576       </vers:VEOIdentifier>
577      </vers:RecordMetadata>
578      <vers:Document vers:id="Revision:1-Document:1">
579       <vers:DocumentMetadata>
580        <vers:DocumentAgent>
581         <vers:Text>
582          Author: Andrew Waugh
583         </vers:Text>
584        </vers:DocumentAgent>
585        <vers:DocumentTitle>
586         <vers:Text>
587          Report
588         </vers:Text>
589        </vers:DocumentTitle>
590        <vers:DocumentDate>
591         <vers:Text>
592          2003-03-20T23:24:06-10:00
593         </vers:Text>
594        </vers:DocumentDate>
595        <vers:DocumentSource>
596         <vers:Text>
597          Microsoft Word 97
```

```
598          </vers:Text>
599         </vers:DocumentSource>
600        </vers:DocumentMetadata>
601        <vers:Encoding vers:id="Revision:1-Document:1-Encoding:1">
602         <vers:EncodingMetadata>
603          <vers:FileEncoding>
604           <vers:Text>
605  The content of the DocumentData element is a PDF file. The file conforms to
606  'PDF Reference', third edition, Adobe Portable Document Format, Version 1.4,
607  Adobe Systems Incorporated, Addison Wesley, 2001, ISBN 0-201-75839-3
608  (http://partners.adobe.com/asn/developer/acrosdk/docs/filefmtspecs/PDFReference.pdf
609  visited 7 January 2003) as modified in the 'Errata for PDF Reference, third
610  edition' (http://partners.adobe.com/asn/developer/acrosdk/docs/PDF14errata.txt
611  visited 7 January 2003). It may contain digital signatures defined by PDF
612  Public-key Digital Signature and Encryption Specification, Version 3.2, Jim
613  Pravetz, 12 September 2001, Adobe Systems Incorporated
614  (http://partners.adobe.com/asn/developer/pdfs/tn/ppk_pdfspec.pdf visited
615  28 March 2003) and the appearance of the digital signature in a PDF document
616  is defined in Digital Signature Appearances for Public-Key Interoperability,
617  Adobe Systems Incorporated, September 2001
618  (http://partners.adobe.com/asn/developer/pdfs/tn/PPKAppearances.pdf visited
619  28 March 2003). The file has been encoded using Base64 which is defined in
620  IETF RFC 2045 "Multipurpose Internet Mail Extensions (MIME) Part One:
621  Format of Internet Message Bodies", Section 6.8
622  "Base64 Content-Transfer-Encoding".
623           </vers:Text>
624          </vers:FileEncoding>
625          <vers:SourceFileIdentifier>
626           P:\Presentations\PublicAccountsCtee\VERSIntegrity.pdf
627          </vers:SourceFileIdentifier>
628          <vers:FileRendering>
629           <vers:RenderingText>
630            <vers:Text>
631             See the vers:FileEncoding element
632            </vers:Text>
633           </vers:RenderingText>
634           <vers:RenderingKeywords>
635            b64 pdf
636           </vers:RenderingKeywords>
637          </vers:FileRendering>
638         </vers:EncodingMetadata>
639         <vers:DocumentData
640           vers:id="Revision:1-Document:1-Encoding:1-DocumentData">
641  JVBERi0xLjMNJeLjz9MNCjkwIDAgb2JqDTw8IA0vTGluZWFyaXplZCAxIA0vTyA5MiANL0ggWyAx
642  [...]
643  MGQ+PDJjNWViMzQ4YjcyNzU3ZGUxODRjMTVjYTVjMjA2YWRhPl0NPj4Nc3RhcnR4cmVmDTE3Mw0l
644  JUVPRg0=
645        </vers:DocumentData>
646       </vers:Encoding>
647      </vers:Document>
648     </vers:Record>
649    </vers:ObjectContent>
650   </vers:SignedObject>
651      </vers:OriginalVEO>
652     </vers:ModifiedVEO>
653    </vers:ObjectContent>
654   </vers:SignedObject>
655  </vers:VERSEncapsulatedObject>
```

8 References

[Base64] Base64 Content-Transfer-Encoding, Section 6.8, Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, IETF RFC 2045, N. Freed & N. Borenstein, November 1996, http://www.ietf.org/rfc/rfc2045.txt?number=2045 visited 26 March 2003.

[Canon] Canonical XML Version 1.0, W3C Recommendation, 15 March 2001, http://www.w3.org/TR/xml-c14n visited 26 March 2003.

[DSS] Digital Signature Standard (DSS), FIPS PUB 186-2, National Institute of Standards and Technology, US Department of Commerce, 27 January 2000, http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf visited 25 March 2003.

[Namespace] Namespaces in XML, W3C Recommendation, 14 January 1999, http://www.w3.org/TR/1999/REC-xml-names-19990114/ visited 29 January 2003.

[RFC2459] Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Housley, Ford, Polk, and Solo, IETF RFC 2459, January 1999, http://www.ietf.org/rfc/rfc2459.txt?number=2459 visited 26 March 2003.

[RSA] PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, 14 June 2002, ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf visited 24 March 2003.

[SHS] Secure Hash Standard, FIPS PUB 180-2, National Institute of Standards and Technology, US Department of Commerce, 1 August 2002, http://csrc.nist.gov/publications/fips/fips180-2/fip180-2.pdf visited 25 March 2003.