Especificación Técnica

FIEE: Formato de Intercambio de Expedientes Electrónicos

Área de Tecnología - División Arquitectura y Normas

Control de Cambios

Fecha	Versión	Descripción	Autor	Aprobado Por
	1.0	Versión inicial		
20/09/2016	1.3			

Este documento ha sido elaborado por AGESIC (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento)

Tabla de Contenidos

1. Introducción 5

2. Objeto 7

3. Referencias Normativas 8

4. Formato de intercambio 9

4.1 Antecedentes 9

4.2 Diagrama esquemático 10

4.3 Ejemplo de expediente en FIEE 11

4.4 Descripción detallada 14

5. Funcionalidad de la Aplicación de Expediente Electrónico 20

5.1 Introducción 20

5.2 Cambio de Carátula 20

5.3 Firma de los expedientes FIEE 20

5.4 Firma de las firmas anteriores 21

5.5 Despliegue de un expediente FIEE 21

5.6 Procedimiento para firmar 22

5.7 ¿Qué datos se firman? 23

6. Migración de SHA-1 a SHA256 26

6.1 Justificación 26

6.2 Implementación 26

6.3 Cambio en validación exhaustiva 28

6.4 Alcance 28

7. Bibliografía 29

agesic

PRESIDENCIA
REPÚBLICA ORIENTAL DEL URUGUAY

1. Introducción

El objetivo del Formato de Intercambio de Expedientes Electrónicos (FIEE) es definir la forma en que los distintos sistemas de Expediente Electrónico enviarán y recibirán expedientes.

Es importante destacar que desde el punto de vista del relacionamiento entre organismos, el único formato válido para expedientes electrónicos es el FIEE, con independencia de los datos que estén almacenados en el formato propio de la aplicación o de metadatos sobre el expediente que se almacenen por separado del mismo.

Todo sistema de Expediente Electrónico de Uruguay (homologado para trabajar con la Aplicación de Ruteo y Trazabilidad de Expedientes Electrónicos -ARTEE-) dispondrá de un formato estándar, el FIEE, para almacenar y desplegar sus expedientes.

Este documento se estructura en dos partes fundamentales: una primer parte en que se presenta el formato en sí mismo (4

Formato de intercambio) y una segunda parte que describe las funcionalidades que deben implementar las aplicaciones de expediente electrónico para generar, enviar y recibir expedientes en formato FIEE (5 Funcionalidad de la Aplicación de Expediente Electrónico).

2. Objeto

Definir y describir el formato estándar para el Intercambio de Expedientes Electrónicos entre los organismos que integran el Estado uruguayo.

3. Referencias Normativas

Los documentos indicados a continuación son indispensables para la aplicación de este documento. Para las referencias fechadas, se aplican solamente las ediciones citadas. Para las referencias sin fecha, se aplican las ediciones más recientes del documento normativo citado (incluyendo cualquier modificación).

El Formato de Intercambio de Expedientes Electrónicos (FIEE) se basa en estándares de amplia adopción: PDF (Norma ISO 32000-1), en particular en la definición de PDF/A para el almacenamiento de documentos electrónicos a largo plazo, plasmado originalmente en la Norma ISO 19005-1:2005 y MIME (Norma ISO/IEC 21000-9:2005/Amd 1:2008) con su extensión segura S/MIME.

4. Formato de intercambio

4.1 Antecedentes

El Formato de Intercambio de Expedientes Electrónicos se basa fuertemente en dos estándares de amplia adopción: PDF (Norma ISO 32000-1), en particular en la definición de PDF/A para el almacenamiento de documentos electrónicos a largo plazo, plasmado originalmente en la Norma ISO 19005-1:2005 y MIME con su extensión segura S/MIME (Especificación RFC 2633).

Un expediente consiste en un objeto MIME multipartes, que contiene:

- Una parte para la carátula, compuesta de un objeto S/MIME multipart/signed que contiene
    - La carátula original en un PDF codificado base64.
    - La(s) firma(s) correspondiente(s).
    - (Opcional) Las carátulas generadas a partir de los sucesivos cambios de carátula, cada una de ellas con la(s) firma(s) correspondiente(s).
- Una parte para cada actuación, compuesta de un objeto S/MIME multipart/signed que a su vez contiene:
    - La actuación propiamente dicha en un PDF codificado base64.
    - La(s) firma(s) correspondiente(s).
    - Un objeto S/MIME de tipo "signed-only" que contiene la firma digital de la firma de la carátula original y de las firmas a las modificaciones de la carátula que existieran, así como de todas las firmas de las actuaciones, firmado con la clave del funcionario actuante.

Dado que las firmas se realizan siempre en el cliente, para reducir el tiempo de transferencia siempre se firma un hash SHA256 del objeto a firmar. En todo el documento cuando se indica **“se firma el objeto”** quiere decir **“se realiza un hash del objeto con el algoritmo SHA256 y se firma el hash”**.

Cuando un expediente en formato FIEE se almacena en un archivo, este deberá llevar la extensión *.fiee* .

4.2 Diagrama esquemático

Usando pseudo-código S/MIME un expediente electrónico se verá de la siguiente forma:

```
-- frontera
      -- caratula
            Datos de la carátula original:
                  FIEE-caratula-version
                  FIEE-caratula-folios
                  FIEE-fecha
                  FIEE-numero-expediente
            Carátula original en PDF
            Firma de la carátula original
      -- caratula
            Datos de la carátula modificada 1:
                  FIEE-caratula-version
                  FIEE-caratula-folios
                  FIEE-fecha
                  FIEE-numero-expediente
            Carátula modificada 1 en PDF
            Firma de la Carátula modificada 1
      -- caratula
      Hash de la carátula
-- frontera
      -- actuacion
            Datos de la actuación 1:
                  FIEE-caratula-version
                  FIEE-folio-inicio
                  FIEE-folio-fin
                  FIEE-fecha
            Contenido de la actuación 1 en PDF
            Firma de la actuación 1
            Firma de las firmas anteriores
      -- actuacion
            Datos de la actuación 2:
                  FIEE-caratula-version
                  FIEE-folio-inicio
                  FIEE-folio-fin
                  FIEE-fecha
            Contenido de la actuación 2 en PDF
            Firma de la actuación 2
            Firma de las firmas anteriores
      -- actuacion
            Datos de la actuación 3:
                  FIEE-caratula-version
                  FIEE-folio-inicio
                  FIEE-folio-fin
                  FIEE-fecha
            Contenido de la actuación 3 en PDF
            Firma de la actuación 3
            Firma de las firmas anteriores
      -- actuacion
-- frontera
```

4.3 Ejemplo de expediente en FIEE

Los elementos que componen un expediente almacenado en el formato FIEE se muestran a continuación con un ejemplo (las codificaciones están solamente a modo de ejemplo).

```
MIME-version: 1.0
FIEE-version: 1.2.2
Content-Type: multipart/mixed;
      boundary="Expediente"

--Expediente
Content-Type: multipart/mixed;
      boundary="Caratula"

--Caratula
Content-Type: multipart/signed; protocol="application/pkcs7-
signature";micalg=sha256;
      boundary="caratula0Doc"

--caratula0Doc
Content-Type: application/pdf; name="car0.pdf";
      FIEE-caratula-version="0";
      FIEE-caratula-folios="0";
      FIEE-fecha="20140225133717000";
      FIEE-numero-expediente="2014-10-1-0000041"
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="car0.pdf"

JVBERi0xLjQKJeLjMiAwIG9iaiA8PC9JbnRlbnQvUGVyY2VwdHVhbC9EZWNvZGVQYXJtczw8
L0NvbG9ycyAzL1ByY3RvciAxNS9CaXRzUGVyQ29tcG9uZW50IDgvQ29sdW1ucyAzMTE+Pi9U
eXBlL1hPYmplY3Qvsb3JTcGFjZVsvQ2FsUkdCPDwvTWF0cml4WzAuNDEyMzkgMC4yMTI2NCA
--caratula0Doc
Content-Type: text/plain; name="hash_car0";
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="hash_car0"

df9aeb3a59d1e1d3f80e1c127a9d2c8ddb5b668850fda5cbb31676a99bfc5309
--caratula0Doc
Content-Type: application/pkcs7-signature; name="car0.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="car0.p7s"

MIIIKwYJKoZIhvcNoIIIHDCCCBgCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCBf0w
ggX5MIIE4aADAgECgd0VAAAAAB/qMA0GCSqGSIb3DQEBBQUAMGIxEzARBgoJkiaJk/IsZAEZ
FgNjb20xEjAQBgoJk/IsZAEZFgJzdDEbMBkGCgmSJomT8ixkARkWC2V4cGVkaWVudGVzMRow
--caratula0Doc--

--Caratula
Content-Type: multipart/signed; protocol="application/pkcs7-
signature";micalg=sha256;
      boundary="caratula1Doc"

--caratula1Doc
Content-Type: application/pdf; name="car1.pdf";
      FIEE-caratula-version="1";
      FIEE-caratula-folios="0";
```

```
      FIEE-fecha="20140226114620000";
      FIEE-numero-expediente="2014-10-1-0000041";
Content-Transfer-Encoding: base64
Content-Disposition: inline;
      filename="car1.pdf"

JVBERi0xLjLjz9MKMiAwIG9iaiA8PC9BbHRlcm5hdGUvRGV2aWNlUkdCL0xlbmd0aCAyNTk1
L04gMy9GaWASx0ZXIvRmxhdGVEZWNvZGU+PnN0cmVhbQp4nJ2Wd1RU1xaHz713eqHNMBQpC9
N6nSRGGYGWAozNLEhogIRRUQEFUGCIgaMhiKxIoqFgGDBHpAgoMRgFFFReTOyVnTl5bXl98f
--caratula1Doc
Content-Type: text/plain;
      name="hash_car1";
Content-Transfer-Encoding: base64
Content-Disposition: inline;
      filename="hash_car1"

d6f4a1ae0214943700def97b33b1f29cf4115ee14dfd7a1dd05ca6afdb970653
--caratula1Doc
Content-Type: application/pkcs7-signature; name="car1.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="car1.p7s"

MIIIKwYJKoZIAQcCoIIIHDCCCBgCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCBf0w
ggX5MIIE4aADAgoagd0VAAAAAB/qMA0GCSqGSIb3DQEBBQUAMGIxEzARBgoJkiaJk/IsZAEZ
FgNjb20xEjAQkiaJk/IsZAEZFgJzdDEbMBkGCgmSJomT8ixkARkWC2V4cGVkaWVudGVzMRow
--caratula1Doc--

--Caratula--

--Expediente
Content-Type: multipart/mixed;
      boundary="actuacion1"

--actuacion1
Content-Type: multipart/signed; protocol="application/pkcs7-signature";
micalg=sha256;
      boundary="actuacion1doc"

--actuacion1doc
Content-Type: application/pdf; name="act1.pdf";
      FIEE-caratula-version="0";
      FIEE-folio-inicio="1";
      FIEE-folio-fin="1";
      FIEE-fecha="20140226114143139";

Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="act1.pdf"

JVBERi0xLjQKJeLjz9AwIG9iajw8L0Jhc2VGb250L1RpbWVzLUJvbGRJdGFsaWMvVHlwZS9G
b250L0VuY29kaW5nL1Fuc2lFbmNvZGluZy9TdWJ0eXBlL1R5cGUxPj4KZW5kb2JqCjIgMCBv
Ymo8PC9CYXNlRm9udC1lcy1Cb2xkL1R5cGUvRm9udC9FbmNvZGluZy9XaW5BbnNpRW5jb2Rp
--actuacion1doc
Content-Type: text/plain; name="hashact1";
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="hashact1"

a2913beb8ba2b2ff44fa200fb640e19634fce0c813876cf089bb31bf9521d108
--actuacion1doc
```

```
Content-Type: application/pkcs7-signature;
      name="act1fir1.p7s";
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename="act1fir1.p7s"

MIIIKwYJKoZIhvcNAQIIHDCCCBgCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCBf0w
ggX5MIIE4aADAgECAg0VAAAAAB/qMA0GCSqGSIb3DQEBBQUAMGIxEzARBgoJkiaJk/IsZAEZ
FgNjb20xEjAQBgoJkiIsZAEZFgJzdDEbMBkGCgmSJomT8ixkARkWC2V4cGVkaWVudGVzMRow
--actuacion1doc
Content-Type: application/pkcs7-signature; name="act1fir2.p7s";
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=" act1fir2.p7s"

MIIIKwYJKoZIhvcNAQIIHDCCCBgCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCBf0w
ggX5MIIE4aADAgECAg0VAAAAAB/qMA0GCSqGSIb3DQEBBQUAMGIxEzARBgoJkiaJk/IsZAEZ
FgNjb20xEjAQBgoJkiIsZAEZFgJzdDEbMBkGCgmSJomT8ixkARkWC2V4cGVkaWVudGVzMRow
--actuacion1doc--

--actuacion1
Content-Type: application/pkcs7-mime; smime-type=signed-data;
name="actfirs.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="actfirs.p7m"

MIIIKwYJKoZIhvcNAQIIHDCCCBgCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCBf0w
ggX5MIIE4aADAgECAg0VAAAAAB/qMA0GCSqGSIb3DQEBBQUAMGIxEzARBgoJkiaJk/IsZAEZ
FgNjb20xEjAQBgoJkiIsZAEZFgJzdDEbMBkGCgmSJomT8ixkARkWC2V4cGVkaWVudGVzMRow
--actuacion1--

--Expediente
Content-Type: multipart/mixed;
      boundary="actuacion2"

--actuacion2
Content-Type: multipart/signed; protocol="application/pkcs7-signature";
micalg=sha256;
      boundary="actuacion2doc"

--actuacion2doc
Content-Type: application/pdf; name="act2.pdf";
      FIEE-caratula-version="0";
      FIEE-folio-inicio="2";
      FIEE-folio-fin="2";
      FIEE-fecha="20140226114453571";

Content-Transfer-Encoding: base64
Content-Disposition: inline;
      filename="act2.pdf"

JVBERi0xLjQKJeLjz9AwIG9iajw8L0Jhc2VGb250L1RpbWVzLUJvbGRJdGFsaWMvVHlwZS9G
b250L0VuY29kaW5nL1Fuc2lFbmNvZGluZy9TdWJ0eXBlL1R5cGUxPj4KZW5kb2JqCjIgMCBv
Ymo8PC9CYXNlRm9udC1lcy1Cb2xkL1R5cGUvRm9udC9FbmNvZGluZy9XaW5BbnNpRW5jb2Rp
--actuacion2doc
Content-Type: text/plain;
name="hashact2";
Content-Transfer-Encoding: base64
Content-Disposition: inline;
```

```
      filename="hashact2"

a2913beb8ba2b2ff44fa200fb640e19634fce0c813876cf089bb31bf9521d108
--actuacion2doc
Content-Type: application/pkcs7-signature;
name="act2.p7s";
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename="act2.p7s"

MIIIKwYJKoZIAQcCoIIIHDCCCBgCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCBf0w
ggX5MIIE4aADAgoagd0VAAAAAB/qMA0GCSqGSIb3DQEBBQUAMGIxEzARBgoJkiaJk/IsZAEZ
FgNjb20xEjAQkiaJk/IsZAEZFgJzdDEbMBkGCgmSJomT8ixkARkWC2V4cGVkaWVudGVzMRow
--actuacion2doc--

--actuacion2
Content-Type: application/pkcs7-mime; smime-type=signed-data;
name="act2firs.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename="act2firs.p7m"

MIIIKwYJKoZIAQcCoIIIHDCCCBgCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCBf0w
ggX5MIIE4aADAgoagd0VAAAAAB/qMA0GCSqGSIb3DQEBBQUAMGIxEzARBgoJkiaJk/IsZAEZ
FgNjb20xEjAQkiaJk/IsZAEZFgJzdDEbMBkGCgmSJomT8ixkARkWC2V4cGVkaWVudGVzMRow
--actuacion2--

--Expediente--
```

4.4 Descripción detallada

A continuación se describen los elementos que componen el expediente.

4.4.1 Fronteras (*boundarys*)

Los *strings* utilizadas se incluyen a modo de ejemplo. Cada expediente puede utilizar las fronteras que crea conveniente, siempre que cumplan con el estándar. Se recomienda utilizar textos auto explicativos para los *boundary*s, de modo de que en caso de ser necesario facilitar la revisión del código fuente.

La primer parte contiene la carátula original y las sucesivas modificaciones (en el ejemplo separada entre el *boundary*), la segunda parte contiene cada una de las actuaciones.

4.4.2 Cabezal MIME

Es un cabezal de un objeto MIME sin ninguna particularidad especial. Incluye un atributo con la versión de FIEE que se está utilizando y debe obligatoriamente tener como tipo *"multipart/mixe*d", para indicar que el objeto tiene varias partes complementarias y que son de tipos distintos.

```
MIME-version: 1.0
FIEE-version: 1.2.2
Content-Type: multipart/mixed;
      boundary="Expediente"
```

4.4.3 Carátula

4.4.3.1 Cabezal de la carátula

Indica que la primera parte contiene un objeto MIME. También es obligatorio que contenga el tipo "multipart/mixed".[1]

```
--Expediente
Content-Type: multipart/mixed;
      boundary="Caratula"
```

4.4.3.2 Carátula original

Todo expediente en formato FIEE tiene obligatoriamente una carátula original, que es la primera que aparece en la parte MIME que contiene la carátula. La carátula original está firmada por el(los) funcionario(s) actuante(s) pero no contiene la firma de las firmas anteriores.

4.4.3.3 Cabezal del PDF de la carátula

Indica que sigue un nuevo objeto MIME, en este caso de tipo "*multipart/signed*", siguiendo el estándar S/MIME.

```
--Caratula
Content-Type: multipart/signed; protocol="application/pkcs7-signature";
micalg=sha256;
      boundary="caratula0Doc"
```

4.4.3.4 Objeto PDF de la carátula

Es el PDF/A que representa la caratula codificado en base64.

```
--caratula0Doc
```

[1] Dado que la carátula no tiene la necesidad de firmar las firmas anteriores, el objeto MIME podría ser más sencillo, obviando este nivel de anidación. Se decidió sin embargo mantenerlo para que todos los objetos que contiene el expediente sean idénticos en su estructura.

```
Content-Type: application/pdf; name="car0.pdf";
      FIEE-caratula-version="0";
      FIEE-caratula-folios="0";
      FIEE-fecha="20140225133717000";
      FIEE-numero-expediente="2014-10-1-0000041"
Content-Transfer-Encoding: base64
Content-Disposition: inline;
      filename="car0.pdf"

JVBERi0xLjQKJeLjMiAwIG9iaiA8PC9JbnRlbnQvUGVyY2VwdHVhbC9EZWNvZGVQYXJtczw8
L0NvbG9ycyAzL1ByY3RvciAxNS9CaXRzUGVyQ29tcG9uZW50IDgvQ29sdW1ucyAzMTE+Pi9U
eXBlL1hPYmplY3Qvsb3JTcGFjZVsvQ2FsUkdCPDwvTWF0cml4WzAuNDEyMzkgMC4yMTI2NCA
```

Se agregaron parámetros al atributo "Content-Type", específicos del FIEE:

- **FIEE-caratula-version:** número de versión de la carátula, 0 es obligatorio para la original, que va siempre en primer lugar, y 1, 2, 3, etc. para las subsiguientes.
- **FIEE-caratula-folios:** número de folios que ocupa la carátula. La numeración de la carátula es independiente de la numeración de las actuaciones.
- **FIEE-fecha:** fecha de la creación de la carátula, que en el caso de la carátula original coincide con la creación del expediente, en formato *aaaammddhhmmss.*
- **FIEE-numero-expediente:** número asignado por el organismo para el expediente, preferiblemente, pero no obligatoriamente, en el formato *aaaa-ii-uuu-nnnnnn* donde *aaaa* corresponde al año, *ii* al inciso, *uuu* a la unidad ejecutora y *nnnnnn* al número de expediente.

4.4.3.5 Hash de la carátula (opcional)

A continuación del PDF con la carátula, sigue el *hash* de la misma. El mismo debe generarse utilizando el algoritmo *SHA256*. Puede verse el ejemplo seguidamente.

```
Content-Type: text/plain; name="hashcar0";
Content-Transfer-Encoding: base64
Content-Disposition: inline;
      filename="hashcar0"

df9aeb3a59d1e1d3f80e1c127a9d2c8ddb5b668850fda5cbb31676a99bfc5309
```

4.4.3.6 Firma de la carátula

A continuación del hash, sigue la firma según el estándar S/MIME. La firma no es la firma del PDF en base64 propiamente dicho sino de un *hash* del mismo generado con el algoritmo *SHA256*, especificado anteriormente. **La firma deberá incluir el certificado del firmante.**

```
--caratula0Doc
Content-Type: application/pkcs7-signature;
```

```
name="car0.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename="car0.p7s"

MIIIKwYJKoZIhvcNoIIIHDCCCBgCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCBf0w
ggX5MIIE4aADAgECgd0VAAAAAB/qMA0GCSqGSIb3DQEBBQUAMGIxEzARBgoJkiaJk/IsZAEZ
FgNjb20xEjAQBgoJk/IsZAEZFgJzdDEbMBkGCgmSJomT8ixkARkWC2V4cGVkaWVudGVzMRow
```

4.4.3.7 Modificaciones a la carátula (opcional)

Si se realizan modificaciones a la carátula, las carátulas subsiguientes se agregan como nuevas partes a continuación de la original, tal como se muestra en el código de ejemplo (véase apartado 4.3 Ejemplo de FIEE).

Al igual que la carátula original, las modificaciones están firmadas por el funcionario actuante, pero a diferencia de las actuaciones, no contienen la firma de las firmas anteriores.

4.4.4 Actuación

4.4.4.1 Cabezal de la Actuación

A continuación de la carátula viene la primera actuación. El cabezal, como todos los cabezales de actuaciones debe tener el tipo "*multpart/mixed*"

```
--frontera
Content-Type: multipart/mixed;
      boundary="actuacion1"
```

4.4.4.2 Cabezal del PDF de la Actuación

Indica que sigue un nuevo objeto MIME, en este caso de tipo "*multipart/signed*", siguiendo el estándar S/MIME.

```
--actuacion1
Content-Type: multipart/signed; protocol="application/pkcs7-signature";
micalg=sha256;
      boundary="actuacion1doc"
```

4.4.4.3 Objeto PDF de la Actuación

Es el PDF/A de la actuación codificado en base64.

```
--actuacion1doc
Content-Type: application/pdf; name="act1.pdf";
      FIEE-caratula-version="0";
      FIEE-folio-inicio="1";
      FIEE-folio-fin="1";
      FIEE-fecha="20140226114143139";
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="act1.pdf"
```

```
JVBERi0xLjQKJeLjz9AwIG9iajw8L0Jhc2VGb250L1RpbWVzLUJvbGRJdGFsaWMvVHlwZS9G
b250L0VuY29kaW5nL1Fuc2lFbmNvZGluZy9TdWJ0eXBlL1R5cGUxPj4KZW5kb2JqCjIgMCBv
Ymo8PC9CYXNlRm9udC1lcy1Cb2xkL1R5cGUvRm9udC9FbmNvZGluZy9XaW5BbnNpRW5jb2Rp
```

Se agregaron parámetros al atributo "Content-type", específicos del FIEE:

- **FIEE-caratula-version**: indica la carátula que estaba vigente en el momento de la actuación. Este dato puede ser redundante, pero facilita enormemente la verificación de la cadena de firmas.
- **FIEE-folio-inicio:** folio inicial de la actuación. En la primera actuación debe ser obligatoriamente 1, en las actuaciones subsiguientes debe ser el final de la actuación anterior más 1.
- **FIEE-folio-fin:** número del último folio de la actuación. Debe ser mayor o igual que el folio inicial.
- **FIEE-fecha:** fecha de la actuación en formato *aaaaddmmhhmmss*.

4.4.4.4 Hash de la Actuación (opcional)

A continuación del PDF de la actuación, sigue el hash de la misma. Dicho hash debe generarse utilizando el algoritmo *SHA256*. Puede verse el ejemplo seguidamente.

```
Content-Type: text/plain;
      name="hashact1";
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="hashact1"

a2913beb8ba2b2ff44fa200fb640e19634fce0c813876cf089bb31bf9521d108
```

4.4.4.5 Firma de la Actuación

A continuación del PDF de la actuación, sigue la firma, siguiendo estrictamente el estándar S/MIME. La firma no es la firma del PDF en base64 propiamente dicho sino de un *hash* del mismo generado con el algoritmo *SHA256*. **La firma deberá incluir el certificado del firmante.**

La actuación puede ser firmada más de una vez (n veces), cada firma tiene la misma estructura y firma el mismo hash original de la actuación.

```
--actuacion1doc
Content-Type: application/pkcs7-signature; name="act1fir1.p7s";
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="act1fir1.p7s"

MIIIKwYJKoZIhvcNAQIIHDCCCBgCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCBf0w
ggX5MIIE4aADAgECAg0VAAAAAB/qMA0GCSqGSIb3DQEBBQUAMGIxEzARBgoJkiaJk/IsZAEZ
FgNjb20xEjAQBgoJkiIsZAEZFgJzdDEbMBkGCgmSJomT8ixkARkWC2V4cGVkaWVudGVzMRow
```

En el ejemplo se incluyen 2 firmas para la actuación, después de la frontera correspondiente, se incluye otro objeto MIME de firma, con formato idéntico al anterior:

```
--actuacion1doc
Content-Type: application/pkcs7-signature; name=" act1fir2.p7s";
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=" act1fir2.p7s"

MIIIKwYJKoZIhvcNAQIIHDCCCBgCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCBf0w
ggX5MIIE4aADAgECAg0VAAAAAB/qMA0GCSqGSIb3DQEBBQUAMGIxEzARBgoJkiaJk/IsZAEZ
FgNjb20xEjAQBgoJkiIsZAEZFgJzdDEbMBkGCgmSJomT8ixkARkWC2V4cGVkaWVudGVzMRow
```

4.4.5 Firma de las Carátulas y Actuaciones anteriores

Esta última parte de la actuación contiene la firma digital de todas las firmas (firmas de pdfs), de la carátula original y de las firmas de las modificaciones a la carátula, si existieran, así como de las firmas de todas las actuaciones anteriores del expediente. No debe incluir la firma de la actuación actual o última actuación.

Utiliza el formato "*Signed-only*" del estándar S/MIME, que permite almacenar una firma sin especificar cuál es el contenido firmado. Para generar el contenido a firmar se concatenan todas las firmas anteriores sin los cabezales MIME. Luego se genera un *hash* con el algoritmo *SHA256* y se realiza la firma de ese *hash*.

En el caso de múltiples actuantes, el estándar requiere que sólo uno de ellos firme la firma de las actuaciones anteriores, procedimiento que habitualmente se realiza en el momento del pase del expediente. **La firma deberá incluir el certificado del firmante.**

```
--actuacion1
Content-Type: application/pkcs7-mime; smime-type=signed-data;
      name="act1firs.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename="act1firs.p7m"

MIIIKwYJKoZIhvcNAQIIHDCCCBgCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCBf0w
ggX5MIIE4aADAgECAg0VAAAAAB/qMA0GCSqGSIb3DQEBBQUAMGIxEzARBgoJkiaJk/IsZAEZ
FgNjb20xEjAQBgoJkiIsZAEZFgJzdDEbMBkGCgmSJomT8ixkARkWC2V4cGVkaWVudGVzMRow
```

Las actuaciones siguientes tienen exactamente el mismo formato que la primera, sin excepciones.

5. Funcionalidad de la Aplicación de Expediente Electrónico

5.1 Introducción

En los siguientes apartados se describen las funcionalidades que deben implementar las aplicaciones de expediente electrónico para generar, enviar y recibir expedientes en formato FIEE.

5.2 Cambio de Carátula

El formato FIEE prevé la posibilidad de modificar la carátula original de un expediente. Para ello, la aplicación debe seguir obligatoriamente los siguientes pasos, en el orden indicado:

1. El funcionario realiza las modificaciones a la carátula utilizando la aplicación.
2. Independientemente de la dimensión de los cambios, la aplicación agrega una carátula nueva completa en el lugar correspondiente del expediente en formato FIEE. Modificar la carátula original, así sea para agregar un tilde, rompería la firma que se realizó en el momento de crearla.
3. Agrega una actuación al final del expediente que indique a texto pleno que se modificó la carátula. Puede agregar toda la información adicional que considere relevante. Esta actuación lleva el atributo de versión de carátula con el número de versión de la carátula ya modificada.
4. Tanto la carátula como la actuación se firman siguiendo estrictamente el procedimiento indicado más abajo en el apartado 5.6 “Procedimiento para firmar”.

Este procedimiento, así como la modalidad de almacenamiento tiene por objetivo dar soporte la práctica habitual de cambio de carátula, a la vez que garantiza la integridad del expediente, de la cadena de firmas y el almacenamiento de toda la información: tanto la original como la resultante del cambio.

5.3 Firma de los expedientes FIEE

El formato FIEE exige que cada actuación esté debidamente firmada electrónicamente. Para cumplir con este requisito, es imprescindible que el funcionario actuante firme el expediente en formato FIEE en el mismo momento en que firma la actuación, tanto si el formato de almacenamiento interno de la aplicación es el propio FIEE como si no lo es.

De no ser así, en el momento de requerir un expediente en formato FIEE debería solicitarse nuevamente a cada uno de los actuantes, en el orden indicado, su firma electrónica, algo que es

jurídicamente incorrecto y operativamente inviable. Por este motivo, es recomendable que la aplicación mantenga en paralelo el expediente en su formato interno y en formato FIEE hasta la última actuación firmada.

5.4 Firma de las firmas anteriores

El formato FIEE prevé la inclusión en cada actuación de una firma digital de la carátula vigente al momento de firmar la actuación y de todas las firmas de actuaciones anteriores. Este requisito garantiza la integridad del expediente y la capacidad de reproducir en cualquier momento el expediente no solamente en su estado actual, sino exactamente en el estado en el que estaba cuando un funcionario actuante firmó una actuación anterior.

La firma de las firmas anteriores debe ser realizada por el último funcionario actuante habilitado para firmar electrónicamente. La firma de las firmas anteriores requiere de una única firma electrónica: no está permitido incluir en el documento FIEE más de una firma de firmas anteriores por actuación.

La carátula representa un caso particular para la firma de las firmas anteriores debido a que:

- Las carátulas pueden ser modificadas, las actuaciones no.
- La carátula no lleva firma de firmas anteriores.

Tanto para garantizar la integridad del expediente, como para facilitar el despliegue y la validación de la cadena de firmas, se incluye un atributo específico que numera las versiones de las carátulas. Cada actuación incluye el atributo que indica la versión de la carátula que estaba vigente en el momento en que se actuó.

La firma de las firmas anteriores incluye sólo las firmas de los PDFs de las actuaciones y carátulas (concatenación de firmas de pdfs de actuaciones y carátulas), no de las firmas de firmas.

Para entenderlo llamemos:

- FFAU a la Firma de las Firmas Anteriores de la Última actuación
- FFAOA a la Firma de las Firmas Anteriores de las Otras Actuaciones

La FFAU **NO** incluye las FFAOA.

En la aplicación de Expediente Electrónico la firma de las firmas anteriores implica un procedimiento de firma distinto de la firma de la actuación.

5.5 Despliegue de un expediente FIEE

En todo momento mientras trabaja con un expediente, el usuario de la aplicación debe disponer de la funcionalidad "Desplegar el expediente actual en formato FIEE".

Para ello, la aplicación de expediente electrónico debe seguir obligatoriamente los siguientes pasos, en el orden indicado:

1. Verificar la confidencialidad del expediente y verificar si el usuario tiene derechos suficientes para acceder al mismo. En caso negativo, se aborta el proceso.

2. Generar un único archivo PDF a partir de la última carátula (las demás solo se muestran con el procedimiento de validación exhaustiva y despliegue íntegro -ver más abajo-) y de todas las actuaciones, en el orden en que están almacenadas, foliadas secuencialmente.

3. Foliar. El folio número 1 es el primer folio de la primera actuación. La carátula no se folia si es una única hoja, o se folia de forma independiente en otro caso (por ejemplo con números romanos).

4. Verificar la firma electrónica de la última actuación y la firma de todas las firmas anteriores, correspondiente a la última actuación. En caso de que no verifique, comunicar el error y abortar el proceso. Es recomendable pero no obligatorio validar todas las firmas del documento (véase apartado 5.8 "Validar exhautivamente un expediente FIEE").

5. Desplegar el archivo PDF utilizando el visualizador del navegador Web del equipo del usuario.

5.6 Procedimiento para firmar

El usuario debe comprender cabalmente que el expediente válido es el que se almacena en formato FIEE. Para ello, el procedimiento de firmado debe seguir obligatoriamente los siguientes pasos, en el orden indicado:

1. El usuario indica la acción "Firmar" (por ejemplo, cliqueando un botón).

2. Generar un único archivo PDF siguiendo el procedimiento para el “Despliegue de un expediente FIEE” (5.5 Despliegue de un expediente FIEE).

3. Verificar la firma electrónica de la última actuación y la firma de todas las firmas anteriores, correspondiente a la última actuación. En caso de que no se verifique, comunicar el error y abortar el proceso. Es recomendable pero no obligatorio validar todas las firmas del documento (véase apartado 5.8 "Validar exhaustivamente un expediente FIEE").

4. Generar en PDF la actuación a firmar. El PDF debe incluir TODOS los datos e información que el usuario incorporó a la actuación. Esto incluye todos los adjuntos, sin excepción, que deben generar una salida impresa a PDF. Las páginas deben estar obligatoriamente foliadas, pero no está restringido el formato de las mismas.

5. Agregar al final del PDF de las actuaciones anteriores el de la actuación a firmar (se debe generar y mostrar un único PDF).

6. Desplegar el archivo PDF utilizando el visualizador del navegador Web del equipo del usuario.
7. Habilitar la opción de firma.
8. Realizar la firma de la actuación.

Los documentos ejecutables representan un problema serio para el cumplimiento de las normativas relativas a expedientes electrónicos, ya sea que se almacenen en el propio documento (por ejemplo como *scripts*) o como adjuntos (por ejemplo como un archivo de base de datos). Un documento ejecutable implica que un usuario puede ver dos versiones absolutamente distintas del mismo documento sin que la firma electrónica deje de verificar, ya que lo que se firma es el código ejecutable. A esto se suma que el concepto de foliado que exige la normativa es inconsistente o incompatible con el concepto de ejecución de software.

Es por ello que el FIEE no incluye otro formato de almacenamiento que el PDF.

La aplicación de expediente electrónico es la responsable de garantizar que todo el código que incorpora a los documentos, sea a través de *scripts*, adjuntos o por cualquier otro método, se imprime a PDF de una sola y única forma, siempre idéntica, y de aclarar a los usuarios que más allá de la ejecución que se pueda realizar a partir del código, lo único válido a los efectos del expediente es lo que terminó almacenado en el PDF.

No es obligatorio que la firma de la actuación y la firma de las firmas anteriores se realicen en el mismo momento. Esto se debe a que si una actuación la firma más de un funcionario sería obligatorio que todos firmen a la vez. Una implementación sugerida, pero no obligatoria es que la firma de las firmas anteriores se realice al pasar el expediente. Eventualmente el pase lo podría realizar otro funcionario, siempre que tenga potestades para firmar digitalmente.

5.7 ¿Qué datos se firman?

5.7.1. En una carátula o actuación

Dado que la firma se realiza en el cliente, y con el fin de disminuir la cantidad de información que debe viajar del servidor al cliente, FIEE prevé la firma de un hash generado con el algoritmo SHA256 del objeto a firmar en reemplazo de la firma del propio objeto. Es decir, se firma un hash del PDF en base64 de una carátula o actución.

Esto es válido y obligatorio en todos los casos: carátulas, actuaciones y firma de firmas anteriores.

5.7.2. En la firma de las firmas anteriores

Para la firma de las firmas anteriores es necesario concatenar las firmas anteriores. Ello debe hacerse uniendo el base64 de las firmas según se muestra en el ejemplo.

Firmas incluidas en el expediente:

```
Content-Type: application/pkcs7-signature;
     name="actuacion12.p7s";
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
     filename="actuacion12.p7s"

ZXMgMyAwIFIgDS9NZGr0YSA1IDAgUiANL1BhZ2VMYWJlbHMgMiAwIFIgDT4+IA1lbmRvYmoNNT
AgMCBvYmoNPDMgMzYgL0wgMTQ1IC9GaWx0ZXIgL0ZsYXRlRGVjb2RlIC9MZW5ndGggNTEgMCBS
ID4+IAJlYW0NCkiJYmBg0GFgYPVkYGBg/CjEgA1wQGkBINaCYgYGUQZ+xjzmNawvdBzcGhKA8D
DL
```

```
Content-Type: application/pkcs7-signature;
     name="actuacion13.p7s";
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
     filename="actuacion13.p7s"

jZeo+4RcoDEpExjCNYvc7/7ZhedeD+rqIiPtneeJjq0u6XrMeSR+RFwq98D0b7NsMjYpqdlc+f
1Y7qXg9qn85jlen0yHKdz3xEooyd0OI0XJueQpnxk6hWT0SuYhnOf+3sC7NmSYFvOftCXMbRP0
GPj8eT/sQrzZmmNdb2WtuFyFr7vUat+uaozMoRqo0ATWHMOiMAv6Xcy2lyrbkqtId6Sh9bs1h9
sys3HVXWJRV0cliveaBUytvijmsparpqDIO
```

Objeto a firmar:

```
ZXMgMyAwIFIgDS9NZGr0YSA1IDAgUiANL1BhZ2VMYWJlbHMgMiAwIFIgDT4+IA1lbmRvYmoNNT
AgMCBvYmoNPDMgMzYgL0wgMTQ1IC9GaWx0ZXIgL0ZsYXRlRGVjb2RlIC9MZW5ndGggNTEgMCBS
ID4+IAJlYW0NCkiJYmBg0GFgYPVkYGBg/CjEgA1wQGkBINaCYgYGUQZ+xjzmNawvdBzcGhKA8D
DLjZeo+4RcoDEpExjCNYvc7/7ZhedeD+rqIiPtneeJjq0u6XrMeSR+RFwq98D0b7NsMjYpqdlc
+f1Y7qXg9qn85jlen0yHKdz3xEooyd0OI0XJueQpnxk6hWT0SuYhnOf+3sC7NmSYFvOftCXMbR
P0GPj8eT/sQrzZmmNdb2WtuFyFr7vUat+uaozMoRqo0ATWHMOiMAv6Xcy2lyrbkqtId6Sh9bs1
h9sys3HVXWJRV0cliveaBUytvijmsparpqDIO
```

5.7.3. Validación exhaustiva de un expediente FIEE

Las aplicaciones de expediente electrónico deben proveer una opción para verificar exhaustivamente la validez de las firmas de un expediente en formato FIEE y desplegarlo completo, incluyendo todas las versiones de carátula que contenga.

Esto implica validar la firma de la carátula original y sus modificaciones si existieran, así como las dos firmas correspondientes a cada actuación: la(las) del PDF que contiene la actuación y la que firma las firmas anteriores. Debe validarse una por una las firmas de las actuaciones, en el orden almacenado.

Es importante tomar en cuenta en la validación de la firma de cada actuación qué versión de carátula estaba vigente, e incluir en la validación sólo estas versiones. Para facilitar este proceso cada actuación contiene un atributo específico.

La validación de un expediente FIEE garantiza no solo la integridad del documento, sino además que están presentes todas las actuaciones y que están en el orden en que fueron ejecutadas.

Además de validarlo exhaustivamente, debe proveer la posibilidad de desplegarlo íntegro, incluyendo la carátula original y todas sus modificaciones en el PDF a desplegar.

Tanto el despliegue en formato FIEE como la firma de una actuación en formato FIEE no exigen una validación completa debido a que se presume que puede ser una operación costosa en tiempo. Sin embargo se recomienda hacer todos los esfuerzos necesarios para garantizar una performance de validación que permita realizar una validación completa del expediente tanto al desplegarlo como al firmar una actuación, o al menos en la última de las dos.

No ocurre lo mismo con el despliegue íntegro, que debe ser una opción separada. En el funcionamiento normal, el expediente debe desplegarse mostrando sólo la última versión de carátula.

6. Migración de SHA-1 a SHA256

6.1 Justificación

El avance tecnológico referente a los algoritmos criptográficos hace que cada cierto tiempo la confianza de un determinado algoritmo se vea reducida. Esto obliga a que los sistemas que se basen en la utilización de estos algoritmos tengan que migrar a una versión confiable de los mismos. En esta oportunidad, el Formato de Intercambio de Expediente Electrónico estaba basado en el uso de SHA-1 como algoritmo, y se hace necesario plantear su evolución al algoritmo SHA256.

6.2 Implementación

Como primer punto, el algoritmo *SHA-1* deja de ser soportado por FIEE como algoritmo válido para la firma, sustituyéndose por el algoritmo *SHA256*.

Todos aquellos expedientes que estén firmados utilizando SHA-1 deberán anexar una nueva actuación que contendrá dentro del PDF el texto “Actuación de oficio de seguridad – migración de algoritmo de hash”. A su vez, al Content-Type se le agregará un nuevo parámetro de tipo (FIEE-Actuacion-Seguridad=”1”. Este parámetro indica que la actuación se trata de una actuación de oficio de seguridad.

Salvo por el nuevo parámetro, esta actuación será tratada como cualquier otra y será firmada con el certificado de persona jurídica del organismo. **La firma deberá incluir el certificado del firmante.** Por otro lado, en el lugar donde debería ir la firma de firmas anteriores, se incluirá la firma de un hash de la concatenación de todas las carátulas, firmas de carátulas, actuaciones y firma de actuaciones, en el orden en que ocurren en el FIEE. No se consideraran las firmas de firmas. Es decir, suponiendo que un FIEE contiene:

- Carátula 0 en base 64(C0)
- Firma Carátula 0 en base 64 (FC0)
- Carátula 1 en base 64 (C1)
- Firma Carátula 1 en base 64 (FC1)
- Actuación 1 en base 64 (A1)
- Firma Actuación 1 en base 64 (FA1)
- Actuación 2 en base 64 (A2)
- Firma Actuación 2 en base 64 (FA2)

- Actuación Seguridad en base 64 (AS)

- Firma Actuación Seguridad en base 64 (FAS)

En este caso, siendo H() la fusión de hash (algoritmo SHA256), se deberá formar un hash de la siguiente forma:

H(C0 + FC0 + C1 + FC1 + A1 + FA1 + A2 + FA2 + AS + FAS), siendo "+" la función de concatenación (se debe concatenar ingresando un salto de línea [<CR><LF>] entre elemento y elemento) .

Luego, ese Hash resultante se deberá firmar con el certificado de persona jurídica de la institución, y la firma es la que se incluirá en el lugar donde debería ir la firma de firmas. **La firma deberá incluir el certificado del firmante.**

Una vez realizada esta acción, la evolución del expediente se realizará tal cual se realizaba, teniendo en cuenta que tanto las actuaciones como las carátulas deberán ser firmadas con el algoritmo *SHA256*.

A continuación se presenta un ejemplo de actuación de seguridad a adjuntar (los hash del ejemplo no son válidos):

```
--actuacionSeguridad
Content-Type: multipart/signed; protocol="application/pkcs7-signature";
micalg=sha256;
      boundary="actuacionSeguridaddoc"

--actuacionSeguridaddoc
Content-Type: application/pdf;
name="actuacionSeguridad.pdf";
      FIEE-caratula-version="[VERSIÓN DE CARÁTULA ACTUAL]";
      FIEE-folio-inicio="[FOLIO DE INICIO]";
      FIEE-folio-fin="[FOLIO DE FIN]";
      FIEE-fecha="[FECHA]";
      FIEE-Actuacion-Seguridad="1"
Content-Transfer-Encoding: base64
Content-Disposition: inline;
      filename="actuacionSeguridad.pdf"

JVBERi0xLjQKJeLjz9AwIG9iajw8L0Jhc2VGb250L1RpbWVzLUJvbGRJdGFsaWMvVHlwZS9G
b250L0VuY29kaW5nL1Fuc2lFbmNvZGluZy9TdWJ0eXBlL1R5cGUxPj4KZW5kb2JqCjIgMCBv
Ymo8PC9CYXNlRm9udC1lcy1Cb2xkL1R5cGUvRm9udC9FbmNvZGluZy9XaW5BbnNpRW5jb2Rp
--actuacionSeguridaddoc
Content-Type: text/plain;
      name="hash_actuacionSeguridad";
Content-Transfer-Encoding: base64
Content-Disposition: inline;
      filename="hash_actuacionSeguridad"

wl5eKGzW1f/ROnjfaze+mI/w/68=
--actuacionSeguridaddoc
Content-Type: application/pkcs7-signature;
      name="actuacionSeguridad.p7s";
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename="actuacionSeguridad.p7s"
```

```
MIIIKwYJKoZIhvcNAQIIHDCCCBgCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCBf0w
ggX5MIIE4aADAgECAg0VAAAAAB/qMA0GCSqGSIb3DQEBBQUAMGIxEzARBgoJkiaJk/IsZAEZ
FgNjb20xEjAQBgoJkiIsZAEZFgJzdDEbMBkGCgmSJomT8ixkARkWC2V4cGVkaWVudGVzMRow
--actuacionSeguridaddoc--

--actuacionSeguridad
Content-Type: application/pkcs7-mime; smime-type=signed-data;
      name="actuacionSeguridadfirmaHistorico.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename="actuacionSeguridadfirmaHistorico.p7m"

MIIIKwYJKoZIhvcNAQIIHDCCCBgCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCBf0w
ggX5MIIE4aADAgECAg0VAAAAAB/qMA0GCSqGSIb3DQEBBQUAMGIxEzARBgoJkiaJk/IsZAEZ
FgNjb20xEjAQBgoJkiIsZAEZFgJzdDEbMBkGCgmSJomT8ixkARkWC2V4cGVkaWVudGVzMRow
--actuacionSeguridad--
```

En el caso de actuacionSeguridadfirmaHistorico, la diferencia está en que para generar el contenido a firmar se sigue el proceso descrito anteriormente.

Nota: Es recomendable que antes de hacer la migración de un expediente a SHA256, se realice la validación exhaustiva del documento FIEE.

6.3 Cambio en validación exhaustiva

La validación exhaustiva de los expedientes debe ser realizada de la misma forma que se realizaba anteriormente, con la salvedad de que el algoritmo usado es *SHA256*.

El cambio en el proceso de validación está en que durante la validación, en caso de encontrarse con una actuación de oficio de seguridad (se puede saber por el parámetro FIEE-Actuacion-Seguridad), se debería realizar la misma acción definida en el punto anterior: se deberá hacer un hash con la concatenación de todas las carátulas, firmas de carátulas, actuaciones y firmas de actuaciones (sin incluir firma de firmas) en el orden correcto. Esa concatenación deberá coincidir con el contenido firmado que se encuentra en el FIEE a validar.

6.4 Alcance

Si bien el proceso de migración puede ser paulatino, el mismo deberá finalmente abarcar todos los expedientes FIEE almacenados en los distintos organismos del Estado.

Se recomienda en primer medida migrar todos los expedientes abiertos, y en una segunda etapa la migración de todos los expedientes archivados.

7. Bibliografía

ISO 32000-1, *Document management -- Portable document format -- Part 1: PDF 1.7*

Internet Engineering Task Force (IETF). *S/MIME Version 3 Message Specification (RFC 2633).* Editor B. Ramsdell. Junio 1991. Disponible en Internet: https://www.ietf.org/rfc/rfc2633.txt; última fecha de consulta: 2016-06-09.