GOVERNMENT GAZETTE
HELLENIC REPUBLIC

6 May 2022 SECOND ISSUE Sheet No. **2232**

CONTENTS

DECISIONS

DECISIONS

No.58876 ΕΞ 2022 (1)

'Amendment to Decision No. 79841/ΕΞ2020/24.7.2020 (Government Gazette 3266/B) on the Enactment of the Technical Specifications (TS) Regulation on Organising and Conducting Online Gaming Services/Games of Chance'.

THE MINISTER OF FINANCE

Having regard to:

1. The provisions of:

a) Article 25 to 54 of Law 4002/2011 amending pension legislation for the Public Sector-Regulations for the development and consolidation of public finances-Responsibilities of the Ministries for Finance, Culture and Tourism and Labour and Social Security (Government Gazette 180/A), in particular the provision of

Article 29(3) and Articles 189-203 of Law 4635/2019 on Investing in Greece and other provisions (Government Gazette 167/A);

b) Law 4624/2019 on the Hellenic Data Protection Authority, measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions (Government Gazette 137/A);

c) Articles 13, 18, 19 and 41 of Law 4622/2019 on the Executive State: organisation, operation and transparency of the Government, government bodies and central public administration (Government Gazette 133/A);

d) Law 4557/2018 (Government Gazette 139/A) on the Prevention and suppression of money laundering and terrorist financing (incorporation of Directive 2015/849/EU) and other provisions;

e) Law 3469/2006 (Government Gazette 131/A) on the National Printing House, Government Gazette and Law 4727/2020 entitled 'Digital Governance' (Transposition of Directive 2016/2102/EU into Greek law) and 'Electronic Communications' (Transposition of Directive 2019/1024/EU into Greek law) and other provisions (Government Gazette 184/A), in particular Chapter IA 'Digital Transparency-DIAVGEIA program;

f) Articles 16 to 23 (incl.) of Law 3229/2004 on the Supervision of private insurance, supervision and audit of games of chance, application of the International Accounting Standards and other provisions (Government Gazette 38/A) and as a complement to the aforementioned Articles, the provisions of Law 3051/2002 (Government Gazette 220/A) on Constitutionally established independent authorities, amendment and supplementation of the public sector recruitment system and related regulations;

g) Articles 58 to 60 of Law 2961/2001 on the Ratification of the Code on taxation of inheritance, gifts inter vivos, parental donations and lottery gains (Government Gazette 266/A);

h) Presidential Decree No. 83/2019 (Government Gazette 121/A) on the Appointment of a Deputy Prime Minister, Ministers, Deputy Ministers and Assistant Ministers;

i) Presidential Decree No. 81/2018 on the Transposition of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (consolidated version) (OJ L 241, 17.9.2015, p. 1) and other provisions into Greek law (Government Gazette 151/A);

j) Article 34 of Presidential Decree No. 142/2017 on the Organisational structure of the Ministry of Finance (Government Gazette 181/A);

k) Article 90 of Presidential Decree No. 63/2005 on the Codification of laws on Government and government bodies (Government Gazette 98/A) as in force with Article 119(22) of Law 4622/2019 (Government Gazette 133/A);

l) Joint Ministerial Decision No. 70330οικ./30.6.2015 issued by the Minister of Finance, Infrastructure, Maritime Affairs and Tourism and the Minister of Justice, Transparency and Human Rights, on the adaptation of the Greek legal order in line

with Directive 2013/11/EU as in force (Government Gazette 1421/B);

m) Joint Decision No. 56660/1679/22.12.2011 (Government Gazette 2910/B) issued by the Minister of Finance and the Minister of Culture & Tourism confirming the commencement of the Hellenic Gaming Commission (HGC) operations (Government Gazette 2910/B);

n) Decision No.145940/ΕΞ 2020/21.12.2020 (YODD 1089) issued by the Minister of Finance read in conjunction with similar Decisions No. 2/3935/0004/24.7.2018 (YODD 428), 9433ΕΞ 2019/12.2.2019 (YODD 64), and 3557 ΕΞ 2020/14.01.2020 (YODD 20) on the establishment of the HGC;

o) Decision No. 79841/ΕΞ 2020 (Government Gazette 3266/B) issued by the Minister of Finance on the Enactment of the Technical Specifications (TS) Regulation on the Organisation and Conduct of Online Gaming Services/Games of Chance;

2. The fact that on pages 137 - 138 of the Explanatory Memorandum of Law 4635/2019 (Government Gazette 167/A) is stated, inter alia, that the Gaming Regulation may be adopted by one or more decisions issued by the Minister of Finance, on the recommendation of HGC.

3. Notification with reference number 2019/657/GR of Draft Ministerial Decree on the Enactment of the Technical Specifications (TS) Regulation on the Organisation and Conduct of Online Gaming Services/Games of Chance pursuant to the provisions of Presidential Decree No. 81/2018 (Government Gazette 151/A);

4. Decision No. 613/19.11.2021 by which the HGC recommends to the Minister of Finance the amendment to Decision No. 79841 ΕΞ 2020/24.7.2020 issued by the Minister of Finance on the Enactment of the Technical Specifications (TS) Regulation on the Organisation and Conduct of Online Gaming Services/Games of Chance' (3266/B);

5. The fact that, in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 (OJ L 241), the amendments suggested by this decision do not need to be notified to the EU since they do not restrict already existing and/or notified provisions, nor do they introduce new restrictions, obstacles or prohibitions as to the access, provision, installation and use of gambling services and regarding the specifications for products and services related to such provision and use.

6. The fact that this Decision does not entail any financial burden on the State budget or the HGC budget, we hereby decide:

To amend Decision No.79841/ΕΞ2020/24.07.2020 (Government Gazette 3266/B/) issued by the Minister of Finance on the Enactment of the Technical Specifications (TS) Regulation on the Organisation and Conduct of Online Gaming Services/Games of Chance' as follows:

1. The third subparagraph of Article 7(7.1) shall be amended as follows:

'The License Holder shall notify the HGC of the audit process'.

2. The first and second subparagraph of Article 8(8.4) shall be amended as follows:

'The CIS must employ a mechanism that ensures any critical components contained in the Client Software present on the Player Device and used in conjunction with the CIS are verified-certified upon initiation of any Player Session. The Licence Holder

must notify the HGC of the control program'.

3. Par. 23.2.2 of Article 23 shall be amended as follows:

'23.2.2 Data must be forwarded in the safe storage device (Safe) at least every two (2) hours unless a different recording frequency is specified in a data model'.

4. Par. 23.3.1 of Article 23 shall be amended as follows:

'23.3.1 In order to ensure data integrity and authenticity, data sealing procedure shall include the following steps:

Step 1: Create data packets (batching) containing a number of records, as described in detail in the following sections.

Step 2: Calculation of the hash value (SHA-256) of the current batch.

Step 3: Data compression using a 'deflate' algorithm (RFC1951).

Step 4: Generation of a 256-bit key of the current batch for the encryption of the compressed data.

Step 5: Symmetric encryption of the data batch with the algorithm AES-256 using the key of Step 4.

Step 6: Creation of a manifest and inclusion of metadata.

Step 7: Encryption of the session key of Step 4 with the Authority's public key (RSA-2048).

Step 8: Inclusion of the encrypted session key in the manifest <xenc:EncryptedKey>.

Step 9: Linking of the current data batch to the immediately preceding one (chaining) through the inclusion of a hash (SHA-256) of the latter control batch.

Step 10: Inclusion in the manifest of the hash calculated at Step 2.

Step 11: Digital signature and time-stamping of the manifest of the current batch.

Step 12: Creation and naming of a final zip file.

Step 13: Storage in the Safe.

5. Par. 23.3.1.1 of Article 23 shall be amended as follows:

'23.3.1.1 The data shall be stored in the Safe in the form of data packets (batches). Each batch shall contain only one xml file for each data model. In the event that xml files which belong to different data model need to be sent, then data batches are created as many as the different data models. The data batch shall be time-stamped, as described in paragraph **Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**.

A data batch shall be created according to the recording frequency of the data batch in Safe.

As long as the period of time specified by the recording frequency in Safe for a data batch has elapsed and no records have been stored in the batch, no data batch is created and sent to Safe'.

6. Article 23(23.3.1.2) shall be amended as follows:

'23.3.1.2 In order to ensure a maximum degree of security and maintenance of the logged data, techniques for linking consecutive data batches shall be used before they are permanently stored in the device.

In addition, the chaining process should enhance the integrity and authenticity of recorded data, while ensuring their cohesion.

Through this process, the Authority shall be in a position to detect any deletion or change of stored data, regardless of whether this is considered a fraudulent activity or not.

Upon generation of the current batch, it shall be linked to the immediately preceding one through the inclusion of a hash (SHA-256) of the latter (cryptographic linking).

The way of referencing hash values of previous batches creates a 'chain' of batches, as depicted in the figure below.

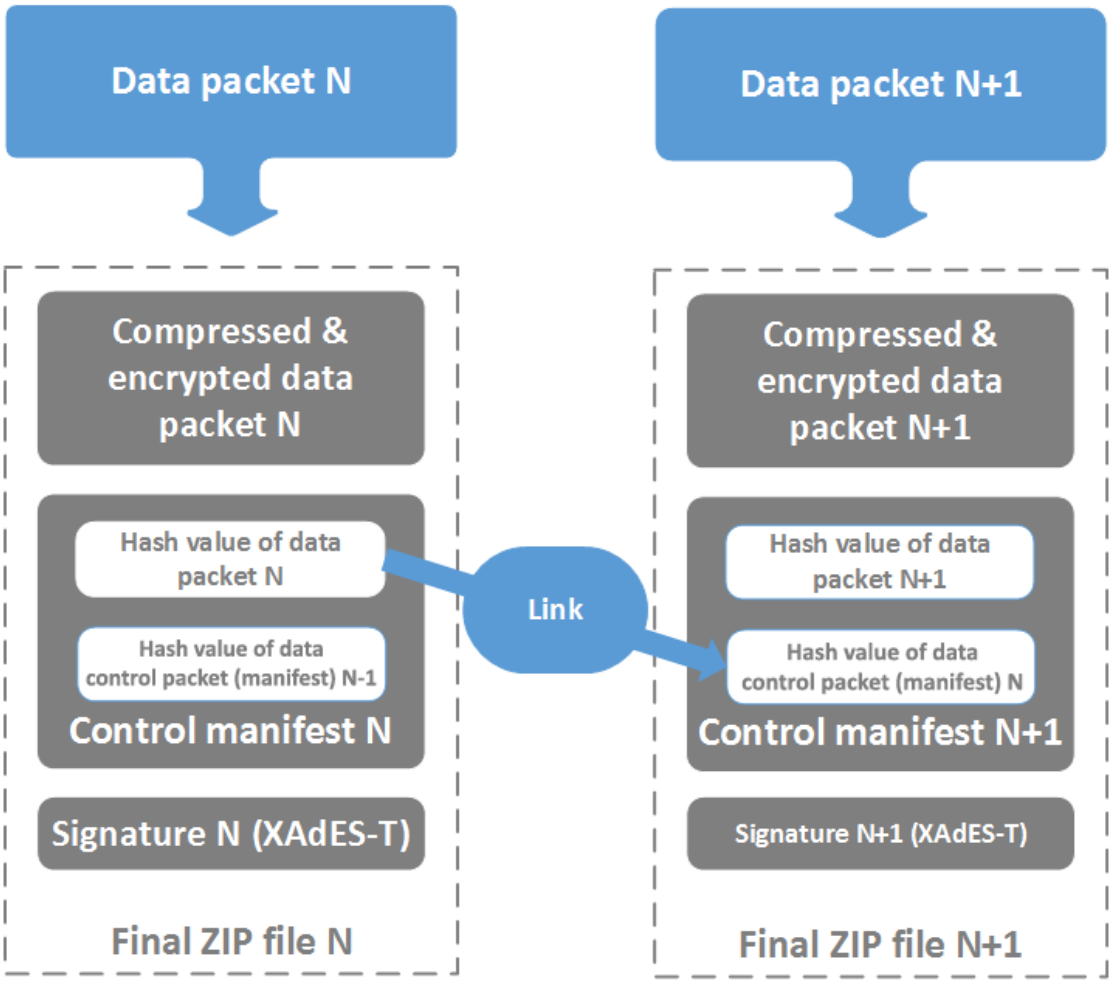

Figure 2. Process of Consecutive Batch Chaining'.

7. Case b of Article 23(23.4.1) shall be amended as follows:

’23.4.1 b) Data storage in the Safe is not allowed, apart from the data modeled or any other files defined by the Authority

8. Article 23(23.4.4) shall be amended as follows:

23.4.4 After the data sealing procedure, the compressed and encrypted data packet shall be stored in the Safe’.

Each data file stored in the Safe shall include the following information:

a) The compressed and encrypted data packet (includes XML data record). This file will always have the name data.bin.

b) The necessary control manifest (described in detail in the relevant section).

The above information shall be stored in zip format in the Safe. The final zip file shall be archived in the Safe in the folder structure of the corresponding day. The name of the resulting file shall be formed in accordance with the following convention:

<licenseholderid>_<serverid>_<seqno>_<xsdnumber>_<YYYYMMDD>_<hhmmss>.zip

where:

<licenseholderid> is the Licence Holder’s registration number as described in the specifications of data batch model;

<serverid>: The name of the server where the file is stored (maximum 10 lowercase characters-numbers. The use of the character "_" is not allowed;

<seqno>: is the data batch sequence number (integer number N>=1);

<xsdnumber>: The number of the data batch as described in the specifications of data batch model;

<hhmmss> is the generation time (24-hour format in UTC).

9. Article 23(23.4.5) shall be amended as follows:
In the safe data storage device, the final data files must be stored in Safe using the following folder structure in accordance with this specific labelling:

<licenseholderid>
o <YYYY>

—————————————<MM>

—————————————<DD>

o <licenseholderid>_<serverid>_1_<xsdnumber>_<YYYYMMDD>_

<hhmmss>.zip

o <licenseholderid>_<serverid>_2_<xsdnumber>_<YYYYMMDD>_

<hhmmss>.zip

o <licenseholderid>_<serverid>_3_<xsdnumber>_<YYYYMMDD>_

<hhmmss>.zip

o …

o <licenseholderid>_<serverid>_N_<xsdnumber>_<YYYYMMDD>

_<hhmmss>.zip

o <YYYY>

———————————————<MM>

———————————————<DD>

o <licenseholderid>_<serverid>_N+1_<xsdnumber>_<YYYYMMD

D>_<hhmmss>.zip

o <licenseholderid>_<serverid>_N+2_<xsdnumber>_<YYYYMMD

D>_<hhmmss>.zip

o <licenseholderid>_<serverid>_N+3_<xsdnumber>_<YYYYMMD

D>_<hhmmss>.zip

o …

o <licenseholderid>_abc15_M_<xsdnumber>_<YYYYMMDD>_<hhmmss>.zip»

10. Article 23(23.4.8) shall be amended as follows:

’23.4.8 The data in the safe data storage device must be securely copied in an alternate storage site, to avoid data loss in case of a major destructive event of the main storage area.

The alternate storage site must be located at a distance of at least 20 kilometres away from the main safe data storage device and be synchronised with it every 30 minutes, through a secure connection dedicated for this purpose. The HGC must also have classified remote access to the alternate storage site (as specified in the relevant section).

The countries/jurisdictions where the alternate storage site is located are defined in the Regulations. The data centre that hosts the alternate storage site infrastructure must meet the specifications described in the ‘IT Infrastructure Security’ Chapter.

In the event of a major destructive event at the main storage site, the time required to restore it to full operation, with all data, and to its former condition, shall not exceed five (5) calendar

days, except in extraordinary events (like natural disasters). In such events, the Licence Holder shall fully justify to the Authority the necessity of extending this limit.

The Licence Holder shall inform the Authority without delay in the event of a major destructive event, justify in detail the causes of the event and submit a plan to restore infrastructure to its former condition.

To initiate data restoration from the alternate storage site to the main one, the Authority's approval is required'.

11. Article 23(23.4.10) shall be amended as follows:

'23.4.10 Where it is necessary to correct data that have already been sent for permanent storage in the safe storage device (Safe), the Licence Holder shall send the new record, keeping a reference to the record to be corrected/cancelled. In particular:

a) Where an existing record must be corrected, a new record is created, with all data of the record to be replaced and a specific reference to it (replaced record id).

b) Where a record must be cancelled, a new record is created that contains only the reference to the cancelled (cancelled record id). For each cancelled record, sufficient justification and time-stamping is required.

Where the amount allocated to a Player is redefined (bet-resettlement), the following shall apply:

In the event when the result of a football game, for example, has been erroneously registered in the Gaming system, and the winnings of one or more bets must be changed, the Licence Holder shall report the difference in the winnings. For example, if the initial record stated that Player A won EUR 100,00 when in fact they won EUR 80,00, a new record will be generated, with the exact same fields, but a winning value of '-EUR 20,00'.

12. The second subparagraph of Article 23(23.6) shall be amended as follows:

'No later than two (2) months after the issuing of HGC Instructions describing in detail the specifications on how to implement the reports, the Licence Holder shall ensure access to said environment by the Authority.

13. Article 23(23.7.2.3.) shall be amended as follows:

'23.7.2.3 The manifest is a supplementary xml file which accompanies each data batch stored in the Safe. It must include all the necessary control information (metadata) of each xml data file contained in each data batch. The most critical information contained in the manifest relates to the identification of the interconnection of successive data batches (chaining hash values), the parameters used for compressing and encrypting data batches and the digital sealing of each data batch stored in the Safe.

In particular, the information contained in the manifest shall be as follows:

a) The unique identifier of the Licence Holder (hgc:licenseholderId);
b) The unique identifier attributed by the Licence Holder to the Server where the file is to be stored (10 lowercase letters-numerals. The use of the character "_" is not allowed. (hgc:serverId).

c) The date and time (UTC) of generation of the manifest (hgc:generationDate);

d) The sequence number of the manifest (hgc:manifestSequenceNumber) which is identical to the sequence number of the data batch;

e) The number of the data model which is included in the data batch (hgc:xsdnumber);

f) The metadata of the xml data file of the data batch (hgc:metadata):

i. Number of records contained in the xml file (hgc:numberOfRecords);
ii. The date and time (UTC) of the first record in the xml file (hgc:datetimeFirstRecord);
iii. The date and time (UTC) of the last record in the xml file (hgc:datetimeLastRecord);
iv. The size of the uncompressed xml data file in bytes (hgc:sizeUncompressed);
v. The size of the compressed file xml data file in bytes (hgc:sizeCompressed);

g) The dynamically generated symmetric key (AES256) with which the data file is asymmetrically encrypted, using the Authority's public key (X.509 certificate), according to the W3C XML Encryption standard (https://www.w3.org/TR/xmlenc-core/) (xenc:EncryptedKey);

h) A reference to the encrypted data, according to the W3C XML Encryption standard (xenc:EncryptedData);

i) The chaining information of consecutive data batches (chaining) (dsig:Manifest);

j) The digital signature of the data batch, including its time-stamping, according to the XAdES standard (dsig:Signature).

Details on the methodology of compiling the xml manifest are shown below.

/hgc:licenseholderId

Unique identifier of the Licence Holder.

/hgc:serverId

Unique identifier attributed by the Licence Holder to the Server where the file is to be stored.

/hgc:generationDate

Date and time (UTC) of generation of the manifest.

/hgc:manifestSequenceNumber

Sequence number of control manifest (whole number N >=1). This is identical to the sequence number of the data batch.

/hgc:xsdnumber

The number of the data model which is included in the data batch.

/hgc:metadata

The metadata of the xml data file of the data batch (aggregated data).

/hgc:metadata/hgc:numberOfRecords

Number of records contained in the xml file.

/hgc:metadata/hgc:dateFirstRecord

Date and time (UTC) of the first record in the xml file.

/hgc:metadata/hgc:dateLastRecord

Date and time (UTC) of the last record in the xml file.

/hgc:metadata/hgc:sizeUncompressed

The size of the non-compressed xml data file in bytes

/hgc:metadata/hgc:sizeCompressed
The size of the compressed xml data file in bytes.

/xenc:EncryptedKey

The *<xenc:EncryptedKey>* element contains a dynamically generated symmetric key (AES256), with which the data file is asymmetrically encrypted, using the Authority's public key (X.509 certificate), according to the W3C XML Encryption standard. The element also contains an ID for the identification of the symmetric key *<xenc: CarriedKeyName>*.

According to the W3C XML Encryption standard, the structure of the specific element shall be as follows:

```
<xenc:EncryptedKey Id="NameOfRegulator"
xmlns="http://www.w3.org/2001/04/xmlenc#">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa1_5"/>
<dsig:KeyInfoxmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<dsig:X509Data>
<dsig:X509SubjectName>CN=Regulator,
OU=Authority</dsig:X509SubjectName>
</dsig:X509Data>
</dsig:KeyInfo>
<xenc:CipherData>
<CipherValue>xyzi…rO+abc</CipherValue>
</xenc:CipherData>
<xenc:CarriedKeyName>K20</xenc:CarriedKeyName>
</xenc:EncryptedKey>
```

In the event that there are more X.509 encryption certifications of the supervisory authority/authorities, then more <xenc:EncryptedKey> elements must be generated, which will contain the same symmetric key and name, but will refer to the Authority's public key (X.509 encryption certification) (ds:X509SubjectName). An identifier will be set for the supervisory authority for which this element is generated as an ID of the <xenc:EncryptedKey> element. The ID will be communicated to the Licence Holder by the Authority.

As name for the identification of the symmetric key <xenc: CarriedKeyName>, the sequence number of the manifest shall be used (e.g., 20), adding the prefix K (Key).

/xenc:EncryptedData

This element represents the report in the encrypted data, according to the XML Encryption standard. It contains the encryption algorithm (AES256) and the internal report to the symmetric key, through its name <xenc: CarriedKeyName>.

The reference to the encrypted data shall be expressed via a URL formed as follows:

a) The URL of the zip file. The path corresponds to the tree structure of the Safe's folders. For Example: <licenseholderid>_<serverid>_<seqno>_<xsdnumber>_<YYYYMMDD>_<hhmmss>.zip
b) The path of the compressed and encrypted data.bin file, within the zip file. For example: /data.bin

An ID shall be added to the final element <xenc:EncryptedData>, based on which the chaining of consecutive patches shall be implemented, as illustrated below in the <dsig:manifest>.

Consequently, the <xenc:EncryptedData>element will have the following structure:

```
<xenc:EncryptedDataxmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="D20">
<xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
<dsig:KeyInfoxmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<dsig:KeyName>K20</dsig:KeyName>
</dsig:KeyInfo>
<xenc:CipherData>
<xenc:CipherReference
URI="/<licenseholderid>/2019/01/01/<licenseholderid>_abc15_20_15_20190101
_155502.zip/data.bin"/>
</xenc:CipherData>
</xenc:EncryptedData>
```

In the aforementioned example, the identification of the <xenc:EncryptedData> element (ID='D20') derives from the sequence number of batch (20), with the addition of prefix D (Data), due to the fact that reference is made to the data batch.

If reference has to be made in the manifest, the relevant sequence number (20) will be used, adding the prefix C (Control).

/dsig:manifest

To chain consecutive batches together, the <dsig:Manifest> element is used. This element derives from the XadES (XMLDSIG) standard. It contains two references to the data (current and previous batch), including their corresponding hash values.

The structure of this element is summarised as follows:

a) It contains a reference to the corresponding <dsig:Manifest> element of the zip batch previously generated, including the hash value of the xml data file generated on the basis of previously canonicalised xml data file (Exclusive XML Canonicalisation [XML-C14N] specification).
   The reference to the encrypted data batch shall be made through a URL formed as follows:
   i. The URL of the previous zip file. The path shall correspond to the tree structure of the Safe's files, as defined in Section 23.4.4. For example:

<licenseholderid>_<serverid>_<seqno>_<xsdnumber>_<YYYYMMDD>_<hhmmss>.zip

   ii. The path of the xml manifest within the previous zip file. For example:

/manifest.xml

   iii. The reference to the Id of the <dsig:Manifest> element of the previous zip batch (<dsig:Manifest id='PreviousID'>). For example:

#<Id>

b) It shall contain a reference to the <xenc:EncryptedData> element of the current manifest, including the hash value of the xml data file generated based on the current canonicalised xml data file (Exclusive XML Canonicalisation [XML-C14N] specification). The hash value is generated from the non-encrypted and uncompressed xml data file.

Then, the conversion rules (decryption, decompression) that must be applied in order to verify the hash value of a data batch must be reported.

Consequently, the <dsig:Manifest>element will have the following structure:

```
<dsig:Manifest Id="C20">
<dsig:ReferenceURI="/<licenseholderid>/2019/01/01/<licenseholderid>_abc15_1
9_15_20190101_145500/manifest.xml#C19">
<dsig:Transforms>
<dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-excc14n#"/>
</dsig:Transforms>
<dsig:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<dsig:DigestValue>PreviousHashValue</dsig:DigestValue>
</dsig:Reference>
<dsig:Reference URI="#D20">
<dsig:Transforms>
<dsig:Transform Algorithm="Decryption algorithm"/>
<dsig:Transform Algorithm="Decompress algorithm"/>
</dsig:Transforms>
<dsig:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<dsig:DigestValue>CurrectHashValue</dsig:DigestValue>
</dsig:Reference>
</dsig:Manifest>
```

/dsig:Signature

This is the element that contains the digital signature of the data batch. A digital signature shall be added as an enveloped signature, according to the XAdES standard, including time-stamping (XAdES-T standard).

14. Article 25(25.5.3) shall be repealed.

In all other cases, provisions of Decision No. 79841 ΕΞ 2020/24.7.2020 (Government Gazette 3266/B) issued by the Minister of Finance shall apply.

This decision shall enter into force as of its publication in the Government Gazette.

This Decision shall be published in the Government Gazette.

Athens, 4 May 2022

Minister

CHRISTOS STAIKOURAS

CORRECTION OF ERRORS

In Decision under Ref. No. 162997(475)/ΠΟ3/6/00009/Σ/ν. 3908/2011/11-04- 2022 issued by the Executive Secretary of the Region of Central Macedonia, published in the Government Gazette (1870/B), on page 18968, in the first column, in the 10th line, above, there is the following correction:

the incorrect point:

"(Main activity code 2008: 25-12-2010)",

shall be corrected as follows:

"(Main activity code 2008: 25.12.10)"

(From the National Printing House)