HELLENIC REPUBLIC

ΑΔΑ: ΩΞΩΨ46ΜΠ3Ζ-Ρ7Τ

POSTED ON THE INTERNET

Greek Government Gazette 3603 B / 24-8-2018

Moschato, 10/ 8 / 2018

POL 1166

To: List of Recipients

ΑΑΔΕ
Independent Authority for Public Revenue (IAPR)

1. DIRECTORATE GENERAL OF ELECTRONIC GOVERNMENT AND HUMAN RESOURCES
DIRECTORATE OF ELECTRONIC SERVICES SUPPORT
DEPARTMENT E
Postal Address : Thessalonikis and Handri 1
ZipCode : 18346 Moschato
Information : P.Mavridis
Phone : 2104802086
Fax : 2104802349
Email : p.mavridis@aade.gr
Url : www.aade.gr

2. INDEPENDENT OFFICE OF SECURITY
Information : D.Tsakiris
Fax : 2104802579
Email : itsecurity@aade.gr

SUBJECT: "Technical specifications of communication and encryption protocol for the transmission of data to the FEM information system"

DECISION

THE GOVERNOR OF THE INDEPENDENT AUTHORITY FOR PUBLIC REVENUE

Taking into consideration:

1. The provisions:

a) of articles 12 par. 9 and 40 of Law 4308/2014 (A' 251) "Greek Accounting Standards, related regulations and other provisions."

b) of article 20 of Law 3842/2010 (A' 58) "Restoration of fiscal justice, tackling tax evasion and other provisions." and in particular of subsection b of paragraph 6 thereof.

c) of A.Y.O. POL.1220/2012 (B' 3517) "Codification – Completion of technical specifications of Fiscal Electronic Mechanisms and systems. Procedures for their use and operation. Specifications of files sent to GSIS.".

d) of A.Y.O. POL 1221/2012 (B' 3513) "Upgrading of support software of the E.A.F.D.S.S. - Determination of sent data files of the tax data in G.S.I.S. pursuant to the provisions of article 20 of Law 3842/2010 (Government Gazette 58/A/23.4.2010)"

e) of the Decision SGPR POL 1068/1-4-2015 (B'497) "Procedures for the approval and revocation of FEMs. Obligations of holders of license of Fiscal Electronic Mechanisms (FEMs), sellers of FEMs, certified technicians of FEMs, holders - users of FEMs."

f) of chapter A "Establishment of an Independent Authority for Public Revenue " of Part One of Law 4389/2016 (A' 94), and in particular paragraphs 1 and 5 of article 14, paragraph 1 of article 2, article 7 and sub-paragraphs 2 and 3 of article 41 thereof.

g) of Δ.ΟΡΓ.Α 1036960 ΕΞ 2017/10-3-2017 (Βʹ 968 and 1238) Decision of the Governor of the Independent Authority for Public Revenue "Organization of the Independent Authority for Public Revenue (IAPR)".

2. The no. 1 of 20-1-2016 Act of the Council of Ministers (YODDD 18) "Selection and appointment of the Secretary General of the Secretariat General for Public Revenue of the Ministry of Finance", in conjunction with the provisions of the first paragraph of par. 10 of article 41 of Law 4389 /2016.

3. The no. Δ6Α 1015213 ΕΞ 2013/28-1-2013 (Βʹ 130 and Βʹ 372) Decision of the Minister of Finance and the Deputy Minister of Finance "Transfer of responsibilities to the Secretary General of the Secretariat General for Public Revenue of the Ministry of Finance", as amended, supplemented and valid, in combination with sub-paragraph a of par. 3 of article 41 of Law 4389/2016.

4. The Δ30Β4008733/1-3-2013 document on "Definition of the communication protocol of the Support Software of the EAFDSSS and the FEM of new specifications with the GSIS. Clarifications on the files sent".

5. Ensuring the privacy of communications (Greek Government Gazette B' 2715/17-11-2011).

6. The fact that, from the provisions of this Decision, no expenditure is incurred against the Budget of the Independent Authority for Public Revenue (IAPR).

WE DECIDE

The definition of specifications for the communication and encryption protocol, which apply on the one hand the information system of the FEMs and on the other hand the FEMs that received approval with the provisions of the technical specifications of POL 1220/2012, all EAFDSSS and the data transmission software of the Electronic Invoicing Provider Services .

Article 1 Definitions - Clarifications

The data transmission software that operates in a Electronic Invoicing Provider of Law 4308/2014 (A΄251) transmits specific data of the sales documents to the information system of FEMs.

For the sake of brevity, in the text of this Decision the term "Data Transmitter (DT)" means the Fiscal Electronic Mechanisms approved by POL 1220/2012, all EAFDSSS and data transmission software operating in Electronic Invoicing Providers.

Access to the Information System of FEM is through the website of IAPR (www.aade.gr), choosing from the tax services: "Businesses - Tax services - Books - Data - Cash registers - Information System of FEM".

Article 2 Encryption algorithm and communication protocol

The DTs encrypt the data to be sent with the symmetric AES-256 encryption algorithm.

The AES key encryption key is provided by the FEM Information System website in the "Business" option. The AES key encryption key is unique per DT.

The encryption is done inside the DT, so that the data is not revealed outside it.

The data to be sent from the DTs are the s.txt files. Their sending url is listed in the FEM information system. The specifications that must be met when sending the data are provided in Appendix A of this decision.

Article 3 Clarifications on the data of transmitted files.

The data transmitted is determined by table C of the POL 1220/2012.

3.1 In particular, regarding the type of sales document field:

In the event that there is withholding tax, the withholding amount will be included as additional information in the sales document type field of the e.txt file (table C of POL 1220/2012) as follows: <type of document> $ <amount> (e.g. .161$100.00, 161#22$100.10).

The retrieval of the above specialized information is done by the EAFDSSS software, in any convenient way. Indicatives can be made, a) through the data line printed on the sales document by the company's commercial software b) by detecting the amount of tax withheld at specific points on the document. The sign of the amount of incidental tax withholding is determined based on table D of POL 1220/2012.

3.2 In the currency code field, a 3-letter code is used in accordance with the international standard ISO 4217. When the euro is used, in the corresponding field of table C of POL 1220/2012 instead of "EUR", the number 0 can alternatively be used.

Article 4 Automatic time synchronization

FEMs have the ability to automatically synchronize the time with the time of the information system of FEMs. The relevant specifications for time synchronization are provided in Appendix B of this decision.

Article 5 Entry into force

This Decision is valid from its publication in the Government Gazette.

This Decision be published in the Government Gazette.

Appendix A : Encryption algorithm and communication protocol specifications

A1. The data is transmitted using telecommunications networks that operate based on the regulation for ensuring the privacy of electronic communications of the Communications Privacy Assurance Authority (Government Gazette B' 2715/17-11-2011).

A2. Transmission occurs after the data file is encrypted using an AES-256 encryption algorithm. As an encryption key, a string with a minimum length of 256 bits issued by the Information System of FEMs for the specific DT is used. and is stored in the information system of the FEM of IAPR.

The information system of FEMs decrypts the data in the same way. The key is retrieved from the FEMs registry of the FEM information system. The reference to the registry is made based on the name of the encrypted file, according to POL 1220/2012.

A3. The communication protocol of the DTs with the FEM information system is the following:

The S.TXT file is encrypted with AES256 in CBC (Cipher Block Chaining) mode and a 16-byte random initialization vector automatically generated by the DT's software and with a key (AES Key) received by the holder of the DT.

The encrypted content is transmitted by HTTP POST multipart form as a file with the name of S.TXT, coded GR-ELOT928, from which the serial number of the DT is derived, which also concerns the Z number submitted. Especially for the transmission software of the Electronic Invoicing Providers, the Z number means the shipping package number.

The transmission contains a field of type TEXT named IV and containing the Hexadecimal representation of the initialization vector (32 HEX characters against the 16 bytes that make up the initialization vector) and a unique field of type FILE with field name "S_TXT_FILE". In the FILE type field "S_TXT_FILE" the value for the file name is the name of the transmitted S.TXT while the value of the file content is the encrypted content of the S.TXT file.

The DT sends the data, implements the HTTP 1.1 protocol and in particular the redirect command that may be sent by the FEM information system in order to transfer the communication to a provider's server.

The FEM information system decrypts the contents of the S.TXT files submitted based on the key it knows and corresponds to the specific DT, and responds with text/plain GR-ELOT928 encoding as follows:

- If everything is in order, the FEM information system responds with the indication OK (Latin characters) and thus confirms the **successful completion of the transmission of the S.TXT file.**
- In the event of an error, the FEM information system responds with 3 fields, separated by a delimiter (;), of which the first is always the ERR indication, the second the error code according to the Error Table, and the third a parameter to explain the error.

Error Table 1

Field 1	Field 2	Field 3
ERR	1 = Wrong S.TXT file name (eg not 31 characters, wrong parts of the name, etc).	
ERR	2 = Wrong S/N DT (e.g. it is not registered in the AADE database, the characters are not Latin, etc.).	
ERR	3= This Z has already been submitted	N=Number of last Z submitted
ERR	4= The previous Z is missing	N= Number of last Z submitted

The return of errors (ERR 1 – 4) from the FEM information system completes the communication unsuccessfully, making the transmission of the S.TXT file inadmissible.

Any other response from the FEM information system is also considered wrong for an unknown reason (eg malfunction of some subsystem of the FEM information system or the provider).

The date of the S.TXT or its lines (e.txt) is not checked, as in real conditions it is possible that a relevant error may occur after (wrong) intervention of a technician in the FEM.

Appendix B: Specifications for synchronizing the time of FEMs with the time of the FEM information system.

As the communication protocol between the FEM information system and the FEMs is HyperText Transfer Protocol (HTTP), the FEMs must read the date and time from the response header of the FEM information system, as provided by RFC7231. Example: Date: Sun, 06 Nov 1994 08:49:37 GMT. It should be noted that the time provided by FEM information system is GMT and therefore FEMs must make the appropriate adjustment to Greek time.

The FEM, after receiving the correct day, hour, minutes and seconds from the FEM information system when communicating with it when Z is issued, adjusts its respective settings, if:

a) The daily receipt counter is 0 (so no new day has been opened) and

b) The received date-time-minutes-seconds sequence has a deviation of up to 30 minutes from the date-time of the last Z of the FEM and

c) The "Automatic time adjustment from SERVER" option in FEM is active.

Especially for the case where the time of the FEM is ahead of the time of the FEM information system, immediately after the synchronization of the time of the FEM during the issuance of report Z, the FEM should be deactivated for as long as necessary, in order not to issue any fiscal receipt with a date and time prior of the last fiscal receipt (Z report included).

THE GOVERNOR

OF THE INDEPENDENT AUTHORITY FOR PUBLIC REVENUE

GEORGIOS PITSILIS