

## Formaty plików przyjmowanych przez system informatyczny GIIF (SI\*GIIF)

System informatyczny Generalnego Inspektora Informacji Finansowej (SI\*GIIF) przyjmuje dane w formacie XML. Kodowanie UTF-8.

### Dane podpisane

SI\*GIIF przyjmuje dane podpisane w formacie CAdES. Przyjmowane są dane w formatach:

- CAdES-E-BES zdefiniowany ETSI EN 319 122-2 V1.1.1 (2016-04)
- CAdES-B zdefiniowany ETSI TS 101 733 V2.2.1 (2013-04)

Należy używać funkcji skrótu SHA-256, SHA-384 lub SHA-512.

### Dane zaszyfrowane

SI\*GIIF przyjmuje dane zaszyfrowane w formacie EnvelopedData zdefiniowanym w RFC-5652.

Wykorzystywana jest technika key transport.

Certyfikat z kluczem publicznym do szyfrowania jest udostępniany pod adresem:

<https://www.giif.mofnet.gov.pl/api/rest2018/certyfikatSzyfrowania>, jeżeli nagłówek Accept jest ustawiony na „application/pkix-cert” to zwrócony zostanie certyfikat w formacie DER, jeśli na „application/x-pem-file” to w formacie PEM.

Dopuszczalny algorytm szyfrowania klucza symetrycznego to: rsaEncryption (PKCS #1)  
OID.1.2.840.113549.1.1.1.

Dopuszczalne algorytmy szyfrowania zawartości to: AES128-CBC i AES256-CBC.

Pole contentType w elemencie encryptedContentInfo powinno zawierać informacje o typie zawartości. To jest „data” OID.1.2.840.113549.1.7.1 dla danych niepodpisanych, „signedData” OID.1.2.840.113549.1.7.2 dla danych podpisanych, lub „compressedData”

OID.1.2.840.113549.1.9.16.9 dla danych skompresowanych. Dopuszczalne jest przekazanie danych podpisanych z contentType ustawionym na „data”.

### Dane skompresowane

Dane mogą zostać skompresowane w sposób opisany w RFC-3274.

## **Sposób przygotowania pliku:**

### **Rejestracja instytucji obowiązanej bez podpisu elektronicznego:**

Plik XML bez podpisu, bez kompresji, bez szyfrowania.

### **Rejestracja instytucji obowiązanej podpisana elektronicznie:**

Plik XML, podpisany CAAdES, bez kompresji, bez szyfrowania.

### **Wykaz transakcji bez podpisu elektronicznego:**

Plik XML, szyfrowanie.

lub

Plik XML, kompresja, szyfrowanie.

### **Wykaz transakcji podpisany elektronicznie:**

Plik XML, podpisany CAAdES, szyfrowanie.

lub

Plik XML, podpisany CAAdES, kompresja, szyfrowanie.