Opis techniczny protokołu komunikacyjnego kasa – Centralne Repozytorium Kas – Standardy kryptograficzne

Właściciel dokumentu	*Ministerstwo Finansów*
Wersja dokumentu	*4.0.0*
Status dokumentu	*dokumentacja*
Data utworzenia	*2017-12-05*
Data modyfikacji	*2021-02-18*
Nazwa pliku	*Opis techniczny protokołu komunikacyjnego kasa – Centralne Repozytorium Kas – Standardy kryptograficzne_v.4.0.0.docx*

Historia zmian

Data	Autor	Podsumowanie zmian	Wersja
2017-12-05	DI	Utworzenie dokumentu.	1.7.8
2018-01-31	DI	Określenie formatu parametru „kid” obiektu JWE.	1.7.9
2018-04-05	DI	Uzupełnienie przykładów weryfikacji komend i danych.	1.8.0
2018-05-15	DI	Ujednolicenie zapisów ze specyfikacją komend.	1.8.1
2018-06-25	DI	Publikacja BIP MF	2.0.0
2020-01-20	DI	Dostosowanie specyfikacji do kas w postaci oprogramowania	3.0.0
2020-04-20	DI	Uzupełnienie przykładów dla kas w postaci oprogramowania	3.0.1
2020-05-05	DI	Uzupełnienie przykładów dla kas w postaci oprogramowania	3.0.2
2021-02-18	CIRF	Dostosowanie specyfikacji do kas rejestrujących online	4.0.0

Spis treści

1 Słownik pojęć używanych w dokumencie

- TLS 1.2 – Transport Layer Security bezpieczny protokół przesyłania danych warstwy aplikacyjnej w wersji 1.2 opisany w dokumencie RFC 5246.
- JSON – JavaScript Object Notation tekstowy format wymiany danych bazujący na podzbiorze języka JavaScript opisany w dokumencie RFC 7159.
- JWS – JSON Web Signature standard tworzenia podpisów cyfrowych dla dokumentów JSON opisany w dokumencie RFC 7515.
- JWE – JSON Web Encryption standard szyfrowania dokumentów bazujących na strukturze JSON opisany w dokumencie RFC 7516.
- JWK – JSON Web Key standard tworzenia struktury klucza kryptograficznego w formacie JSON opisany w dokumencie RFC 7517.
- JWA – JSON Web Algorithms wykaz algorytmów kryptograficznych używanych w JWE i JWS opisany w dokumencie RFC 7518.
- Base64 – kodowanie danych binarnych przy użyciu podzbioru US-ASCII, opisane w sekcji czwartej dokumentu RFC 4648. Zastosowanie takiego formatu pozwala dane binarne umieścić w strukturach danych tekstowych.
- Base64URL – kodowanie danych binarnych z użyciem znaków dozwolonych w adresacji domenowej URL oraz nazewnictwie plików zdefiniowane w sekcji piątej dokumentu RFC 4648. Dodatkowo usuwa się znak dopełnienia '=' z końca zakodowanych danych oraz wszystkie znaki końca linii, spacje i inne dodatkowe białe znaki. Szczegółowa implementacja jest w załączniku C dokumentu RFC 7515.
- Kasa rejestrująca - kasa rejestrująca spełniająca kryteria i warunki techniczne określone w rozporządzeniu Ministra Przedsiębiorczości i Technologii z dnia 28 maja 2018 r. w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące.
- Kasa rejestrująca online - kasa rejestrująca spełniająca wymagania techniczne określone w rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 12 września 2021 r. w sprawie wymagań technicznych dla kas rejestrujących (Dz. U. 2021 r. poz. 1759).
- Kasa rejestrująca w postaci oprogramowania - kasa rejestrująca w postaci oprogramowania spełniająca wymagania techniczne określone w rozporządzeniu Ministra Finansów z dnia 26 maja 2020 r. w sprawie kas rejestrujących mających postać oprogramowania.
- Kasa rejestrująca w postaci urządzenia - kasa rejestrująca lub kasa rejestrująca online.
- Kasa, kasa fiskalna – kasa rejestrująca, kasa rejestrująca online lub kasa rejestrująca w postaci oprogramowania.
- Dane, zbiór danych, dane przesyłane z kasy, dane przesyłane do repozytorium – ustrukturyzowany zestaw dokumentów fiskalnych i niefiskalnych oraz innych danych wygenerowanych przez kasę przesyłany do repozytorium w strukturze umożliwiającej wysłanie wielu dokumentów. Pojęcia danych, danych przesyłanych do repozytorium i zbioru danych są używane zamiennie.
- Dokument w postaci elektronicznej – ustrukturyzowany pojedynczy dokument fiskalny wytworzony przez kasę rejestrującą online lub kasę rejestrującą w postaci oprogramowania opatrzony podpisem kasy przesyłany do repozytorium i na życzenie do klienta – paragon fiskalny w postaci elektronicznej.
- Repozytorium - system teleinformatyczny, prowadzony przez ministra właściwego do spraw finansów publicznych, którego zasadniczym celem jest odbieranie i gromadzenie danych przekazywanych przez kasy rejestrujące i komunikacja z kasami rejestrującymi w zakresie niezbędnym do ich konfiguracji oraz realizowanie innych zadań dla celów kontrolnych i analitycznych. Technicznie Repozytorium zostało zorganizowane jako zespół współpracujących ze

sobą komponentów i składa się z publicznej chmury Azure (Azure WebApi i Azure Event Hub) oraz Serwera CPD i innych komponentów zlokalizowanych w Centrum Informatyki Resortu Finansów.

- Serwer CPD – serwer zlokalizowany w Centrum Informatyki Resortu Finansów, który realizuje wymianę poleceń pomiędzy kasą i repozytorium w szczególności realizuje fiskalizację kasy.
- Azure - chmura publiczna Azure, przez którą przechodzi główny ruch sieciowy pomiędzy kasami a repozytorium. Składa się z dwóch elementów: Azure WebApi oraz Azure Event Hub.
- Azure WebApi - wydzielona logicznie część chmury Azure, z której kasa otrzymuje polecenia np. zmiana harmonogramu komunikacji, zmiana ustawień, żądanie wysłania dodatkowych dokumentów, itp.
- Azure Event Hub - wydzielona logicznie część publicznej chmury Azure, za pośrednictwem której kasa wysyła dane do repozytorium.
- JPKID - niepowtarzalny w ramach pamięci chronionej numer przypisany w kasie do wytworzonego dokumentu, a w kasach mających postać oprogramowania to unikalny kolejny numer wytworzonego dokumentu w ramach numeru pamięci chronionej. Numer pamięci chronionej to numer przypisany fizycznej pamięci chronionej powiązanej z pamięcią fiskalną, ma postać numeryczną liczoną od jeden i maksymalnie trzy cyfry, a w kasach w postaci oprogramowania ma wartość równą jeden. Para wartości 'JPKID' oraz 'pamiecChr' zawartych w strukturze JSON jednoznacznie identyfikują wytworzony przez kasę dokument. Przez wytworzony dokument należy rozumieć wszystkie dokumenty przesyłane przez kasę do repozytorium czyli dokumenty fiskalne, dokumenty niefiskalne oraz zdarzenia. Identyfikator JPKID może mieć postać numeryczną liczoną od jeden i maksymalnie piętnaście cyfr a wraz z numerem pamięci chronionej jednoznacznie identyfikuje dokument wytworzony w kasie i przesłany do repozytorium. Identyfikator JPKID może mieć również postać osiemnastu cyfr otrzymanych przez połączenie znakowo numeru pamięci chronionej "pamiecChr" oraz identyfikatora dokumentu "JPKID" dopełniając obie wartości zerami odpowiednio do trzech i do piętnastu miejsc tak aby wynik składał się z osiemnastu cyfr.

1.1 Wykaz specyfikacji technicznych użytych w dokumencie

Kod	Zagadnienie
RFC 1951	DEFLATE Compressed Data Format Specification version 1.3
RFC 4648	The Base16, Base32, and Base64 Data Encodings
RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2
RFC 7159	The JavaScript Object Notation (JSON) Data Interchange Format
RFC 7515	JSON Web Signature (JWS)
RFC 7516	JSON Web Encryption (JWE)
RFC 7517	JSON Web Key (JWK)
RFC 7518	JSON Web Algorithms (JWA)
RFC 2104	HMAC: Keyed-Hashing for Message Authentication
RFC 3447	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1
RFC 4492	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)
RFC 5289	TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 4055	Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
FIPS 180-4	Secure Hash Standard (SHS)
JOSE	JSON Object Signing and Encryption (JOSE)

2 Zabezpieczenie kanału komunikacyjnego

W komunikacji urządzania fiskalnego z repozytorium do zabezpieczania połączenia sieciowego stosowany jest standard TLSv1.2. Zalecanym algorytmem szyfrowania kanału komunikacyjnego jest algorytm ECDHE_RSA_WITH_AES_128_CBC_SHA256 (kod heksadecymalny {0xC0,0x27}, dziesiętnie 49191) wskazany w dokumencie RFC 5289. Do komunikacji kasy fiskalnej z serwerami opatrzonymi nazwą domenową z sufiksem „.mf.gov.pl" należy użyć uwierzytelniania dwustronnego z wykorzystaniem certyfikatu kasy wystawionego przez zaufanego producenta oraz certyfikatami serwerów wystawionymi przez certyfikat główny ministerstwa. Magazyn certyfikatów kluczy publicznych zaufanych producentów składowany jest w zasobach ministerstwa oddzielnie dla środowiska testowego oraz produkcyjnego. Repozytorium umożliwia zarejestrowanie kilku ważnych certyfikatów danego producenta. W przypadku kompromitacji klucza prywatnego producenta kas certyfikat klucza publicznego skojarzony ze skompromitowanym kluczem prywatnym zostanie usunięty z repozytorium. Klucze kas fiskalnych związane ze skompromitowanym kluczem prywatnym producenta muszą być wymienione. Identyczna sytuacja zaistnieje w przypadku wygaśnięcia ważności certyfikatu klucza publicznego dostarczonego przez producenta.

W komunikacji kasy z usługą EventHub chmury Azure należy użyć uwierzytelniania jednostronnego z wykorzystaniem jednorazowego biletu uwierzytelniającego wygenerowanego dla każdej z kas z określoną ważnością w usłudze Azure WebApi. Certyfikaty repozytorium oraz usług przyjmowania danych do chmury publicznej przekazywane są do urządzanie fiskalnego podczas procesu fiskalizacji zgodnie z dokumentem „Opis techniczny protokołu komunikacyjnego kasa – Centralne Repozytorium Kas – Specyfikacja komend".

3 Certyfikaty kasy fiskalnej

Kasa fiskalna musi posiadać przyporządkowane dwie pary unikalnych kluczy asymetrycznych. Jedna z par kluczy wykorzystywana jest do komunikacji TLS z serwerem CPD oraz chmurą publiczną. Druga para kluczy wykorzystywana jest do podpisywania i szyfrowania wymienianych danych.

Klucze publiczne o długości 2048 bitów muszą być podpisane certyfikatem CA producenta algorytmem RSA z dopełnieniem PKCS1 w wersji 1.5 z wykorzystaniem funkcji skrótu SHA-256 (sha256WithRSAEncryption) wyszczególnionym w sekcji 5 dokumentu RFC 4055, w postaci certyfikatu X.509 w wersji 3 (X.509v3) opisanym w dokumencie RFC 5280.

3.1 Kasy rejestrujące w postaci urządzenia

W kasach rejestrujących w postaci urządzenia wymagane jest umieszczenie w nazwie podmiotu (commonName) tylko numeru unikatowego kasy. Ważność certyfikatu kasy rejestrującej w postaci urządzenia nie może przekroczyć dwudziestu lat (zalecany okres ważności to pięć lat), a data ważności certyfikatu kasy nie może wykraczać poza datę ważności certyfikatu producenta. Poszczególne certyfikaty kas rejestrujących w postaci urządzenia muszą charakteryzować się przynajmniej następującymi cechami oznaczonymi jako krytyczne (critical):

- certyfikat do komunikacji TLS:
  - Key Usage: digitalSignature
  - Extended Key Usage: clientAuth (TLS WWW client authentication)
- certyfikat do podpisywania i szyfrowania:
  - Key Usage: digitalSignature, nonRepudiation, keyEncipherment

Zawartość certyfikatów – wymagania szczegółowe:

- commonName [CN] = **wymagany**

OID description: [2.5.4.3] {joint-iso-itu-t(2) ds(5) attributeType(4) commonName(3)}

- countryName [C] = **wymagany**

OID description: [2.5.4.6] {joint-iso-itu-t(2) ds(5) attributeType(4) countryName(6)}

- organizationName [O] = **wymagany**

OID description: [2.5.4.10] {joint-iso-itu-t(2) ds(5) attributeType(4) organizationName(10)}

- localityName [L] = opcjonalny

OID description: [2.5.4.7] {joint-iso-itu-t(2) ds(5) attributeType(4) localityName(7)}

- stateOrProvinceName = opcjonalny

OID description: [2.5.4.8] {joint-iso-itu-t(2) ds(5) attributeType(4) stateOrProvinceName(8)}

- organizationalUnitName [OU] = opcjonalny

OID description: [2.5.4.11] {joint-iso-itu-t(2) ds(5) attributeType(4) organizationalUnitName(11)}

- emailAddress [E] = opcjonalny

OID description: [1.2.840.113549.1.9.1] {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) emailAddress(1)}

- organizationIdentifier = opcjonalny

OID description: [2.5.4.97] {joint-iso-itu-t(2) ds(5) attributeType(4) organizationIdentifier(97)}

3.2 Kasy rejestrujące w postaci oprogramowania

W kasach rejestrujących w postaci oprogramowania wymagane jest umieszczenie atrybucie nazwa powszechna (commonName) pola podmiot tylko numeru unikatowego kasy oraz w atrybucie numer seryjny (serialNumber) pola podmiot tylko Numeru Identyfikacji Podatkowej (NIP) podatnika używającego kasy poprzedzonego prefiksem „VATPL-". Ważność certyfikatu kasy rejestrującej w postaci oprogramowania nie może być krótsza niż pięć lat i nie może przekroczyć dziesięciu lat, a data ważności certyfikatu kasy nie może wykraczać poza datę ważności certyfikatu producenta. Poszczególne certyfikaty kas rejestrujących postaci oprogramowania muszą charakteryzować się przynajmniej następującymi cechami oznaczonymi jako krytyczne (critical):

- certyfikat do komunikacji TLS:
    - Key Usage: digitalSignature
    - Extended Key Usage: clientAuth (TLS WWW client authentication)
- certyfikat do podpisywania i szyfrowania:
    - Key Usage: digitalSignature, nonRepudiation, keyEncipherment

Zawartość pola podmiot certyfikatów kas – wymagania szczegółowe:

- commonName [CN] = **wymagany**

OID description: [2.5.4.3] {joint-iso-itu-t(2) ds(5) attributeType(4) commonName(3)}

- serialNumber = **wymagany**

OID description: [2.5.4.5] {joint-iso-itu-t(2) ds(5) attributeType(4) serialNumber(5)}

- countryName [C] = **wymagany**

OID description: [2.5.4.6] {joint-iso-itu-t(2) ds(5) attributeType(4) countryName(6)}

- organizationName [O] = **wymagany**

OID description: [2.5.4.10] {joint-iso-itu-t(2) ds(5) attributeType(4) organizationName(10)}

- localityName [L] = opcjonalny

OID description: [2.5.4.7] {joint-iso-itu-t(2) ds(5) attributeType(4) localityName(7)}

- stateOrProvinceName = opcjonalny

OID description: [2.5.4.8] {joint-iso-itu-t(2) ds(5) attributeType(4) stateOrProvinceName(8)}

- organizationalUnitName [OU] = opcjonalny

OID description: [2.5.4.11] {joint-iso-itu-t(2) ds(5) attributeType(4) organizationalUnitName(11)}

- emailAddress [E] = opcjonalny

OID description: [1.2.840.113549.1.9.1] {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) emailAddress(1)}

- organizationIdentifier = opcjonalny

OID description: [2.5.4.97] {joint-iso-itu-t(2) ds(5) attributeType(4) organizationIdentifier(97)}

4 Algorytmy kryptograficzne

Algorytmy kryptograficzne zostały wybrane z listy algorytmów wskazanych w specyfikacji RFC 7518, w której opisano również sposób implementacji danego algorytmu. Za podstawę kryptografii asymetrycznej przyjęto algorytm RSA o długości klucza minimum 2048 bitów, natomiast wykorzystywanym algorytmem symetrycznym jest algorytm AES z blokiem o rozmiarze 128 bitów.

4.1 Podpisywanie

Algorytmem wykorzystywanym do podpisywania komend, zbioru danych i dokumentów elektronicznych przesyłanych pomiędzy kasą i repozytorium jest algorytm RSA z dopełnieniem PKCS1 w wersji 1.5 (RSASSA-PKCS1-v1_5) opisany w sekcji 8.2 specyfikacji RFC 3447 oraz w sekcji 3.3 dokumentu RFC 7518 wraz z funkcją skrótu SHA-256 opisaną w dokumencie FIPS 180-4. W nagłówku JOSE obiektu JWS podpisanych danych JPK w atrybucie „*alg*" symbol algorytmu przyjmie wartość RS256 (”*alg*”:”*RS256*”).

4.1.1 Podpisywanie zbioru danych

W celu weryfikacji po stronie repozytorium autentyczności danych przesyłanych przez kasy w atrybucie „*jpkcertificate*" należy zamieścić certyfikat z kluczem publicznym kasy fiskalnej użytym do podpisania danych, w formacie binarnym DER zakodowanym Base64 bez znacznika początku i końca certyfikatu oraz bez znaków końca linii.

4.1.2 Podpisywanie dokumentu w postaci elektronicznej

W celu weryfikacji po stronie repozytorium autentyczności dokumentów w postaci elektronicznej przesyłanych przez kasy rejestrujące online lub kasy rejestrujące w postaci oprogramowania certyfikat z kluczem publicznym kasy należy zamieścić jako jednoelementową tablicę w atrybucie „*x5c*", w formacie binarnym DER zakodowanym Base64 bez znacznika początku i końca certyfikatu oraz bez znaków końca linii.

4.2 Szyfrowanie symetryczne

Algorytmem wykorzystywanym do szyfrowania podpisanych komend, zbiorów danych i dokumentów w postaci elektronicznej przesyłanych pomiędzy kasą i repozytorium jest algorytm AES z blokiem i kluczem o rozmiarze 128 bitów w trybie CBC z metodą tworzenia kodu uwierzytelnienia wiadomości (MAC - Message Authentication Code) przy użyciu funkcji skrótu (haszowania) SHA-256 opisany w sekcji 5.2.3 dokumentu RFC 7518 (AES_128_CBC_HMAC_SHA_256). W implementacji mechanizmu szyfrowania należy użyć następującej specyfikacji algorytmu AES:

Klucz haszujący	MAC Key Size	16 bytes
Klucz szyfrujący	Encryption Key Size	16 bytes
Tryb szyfru	Cipher Mode	CBC (Chain Block Chaining)
Dopełnienie	Padding	PKCS#7
Rozmiar bloku	Block Size	16 bytes
Wektor inicjujący	Initialization Vector	16 bytes
Kod uwierzytelnienia wiadomości	Message Authentication Code	SHA-256

W nagłówku JOSE obiektu JWE zaszyfrowanych danych w atrybucie „*enc*" symbol algorytmu szyfrującego przyjmie wartość A128CBC-HS256 (”*enc*”: ”*A128CBC-HS256*”).

4.3 Szyfrowanie klucza szyfrującego

Algorytmem wykorzystywanym do szyfrowania klucza szyfrującego jest algorytm RSA z dopełnieniem PKCS1 w wersji 1.5 (RSAES-PKCS1-V1_5) opisany w sekcji 7.2 specyfikacji RFC 3447 oraz w sekcji 4.2 dokumentu RFC 7518. Klucz publiczny do szyfrowania klucza szyfrującego o długości 2048 bitów w postaci certyfikatu X.509 podpisany przez certyfikat główny ministerstwa zostanie udostępniony publicznie oddzielnie dla środowiska testowego oraz produkcyjnego. W nagłówku JOSE obiektu JWE zaszyfrowanych danych w atrybucie „*alg*" symbol algorytmu szyfrującego klucz szyfrujący przyjmie wartość RSA1_5 ("*alg*":"*RSA1_5*"). Dodatkowo w atrybucie „*kid*" należy zamieścić numer seryjny oraz wystawcę certyfikatu użytego do zaszyfrowania klucza szyfrującego. Struktura atrybutu "kid" ma postać dwóch wartości rozdzielonych przecinkiem - numeru seryjnego w postaci szesnastkowej (cyfry i wielkie litery) oraz nazwy wystawcy certyfikatu składającej się tylko z pola 'CN - commonName'.

4.4 Algorytmy kryptograficzne w kasach rejestrujących w postaci oprogramowania oraz kasach rejestrujących online

W kasach rejestrujących online oraz w kasach rejestrujących w postaci oprogramowania wyróżniamy dwa sposoby tworzenia i przesyłania danych do repozytorium. Pierwszy sposób to podobnie jak w kasach rejestrujących zbiory danych zawierające zestaw wielu dokumentów różnego typu. Drugi sposób to pojedyncze dokumenty w postaci elektronicznej. Podział ten jest ściśle określony poprzez opublikowane schematy struktur JSON. W kasach rejestrujących w postaci oprogramowania oraz kasach rejestrujących online występują następujące rodzaje schematów:

- struktura zbioru danych,
- struktura dokumentu w postaci elektronicznej.

W związku z wyodrębnieniem dwóch sposobów tworzenia danych wyróżniamy również dwa podejścia tworzenia podpisu i sumy kontrolnej (skrótu SHA2) poszczególnych dokumentów.

4.4.1 Podpisywanie dokumentów przesyłanych do repozytorium w zbiorach danych

W celu wyliczenia podpisywanego skrótu dokumentu należy połączyć znakowo wyszczególnione dla danego typu dokumentu dane usuwając występujące na początku i na końcu białe znaki oraz przekształcając ciągi znaków do wielkich liter. Elementy niewystępujące należy pominąć i dla powstałego ciągu znaków wyliczyć wartość funkcji skrótu następnie zaszyfrować kluczem prywatnym kasy w sposób opisany w punkcie 4.1. Otrzymaną wartość bajtową należy zamieścić w strukturze JSON w postaci szesnastkowej. Poniżej wyszczególnienie pozycji w odpowiedniej kolejności, które należy użyć do wyliczenia skrótu dla poszczególnych typów dokumentów:

- Raport fiskalny fiskalizacji:
  - NIP
  - nrUnik
  - dataFisk
  - sumaZm
  - serwID
- Raport fiskalny dobowy:
  - NIP
  - nrUnik
  - sprzedBrutto
  - podatekNal
  - zakRap
- Paragon anulowany
  - NIP
  - nrUnik
  - nrDok
  - sumaBrutto
  - zakSprzed
- Dokument niefiskalny
  - NIP
  - nrUnik
  - nrDok
  - zak

Dodatkowo wyszczególnienie pozycji w odpowiedniej kolejności, które należy użyć do wyliczenia skrótu dla poszczególnych typów dokumentów wyłącznie dla kas rejestrujących online:

- Faktura:
  - NIP
  - nrUnik
  - nrDok
  - sumaBrutto
  - zakSprzed
- Faktura anulowana
  - NIP
  - nrUnik
  - nrDok
  - sumaBrutto
  - zakSprzed

Podpisywanie dokumentów w zbiorach danych zaprezentowane jest w załączniku A punkt A.10.1.

4.4.2 Wyznaczanie wartości funkcji skrótu dokumentów przesyłanych w zbiorach danych

W celu wyznaczenia wartości funkcji skrótu dokumentu należy użyć funkcji skrótu SHA-256. Wyznaczenie wartości funkcji skrótu dokumentu przesyłanego w zbiorach danych polega na obliczeniu skrótu SHA2 ze skrótu poprzedniego dokumentu i podpisu bieżącego dokumentu.

Wyznaczanie skrótu dokumentów przesyłanych w zbiorach danych opisane jest w punkcie A.10.2.

4.4.3 Podpisywanie dokumentów w postaci elektronicznej

Podpisywanie dokumentów w postaci elektronicznej realizowane jest z wykorzystaniem obiektów JWS zgodnie ze standardem tworzenia podpisów cyfrowych dla dokumentów JSON opisanym w dokumencie RFC 7515. W sposób szczegółowo opisany w punkcie 5.2.

Podpisywanie dokumentów w postaci elektronicznej szczegółowo opisane jest w punkcie A.10.3.

4.4.4 Wyznaczanie wartości funkcji skrótu dokumentu w postaci elektronicznej

W celu wyznaczenia wartości funkcji skrótu dokumentu w postaci elektronicznej należy użyć funkcji skrótu (haszowania) SHA-256. Wyznaczenie wartości funkcji skrótu dokumentu w postaci obiektu JWS (**paragon fiskalny w postaci elektronicznej**) polega na obliczeniu wyniku funkcji SHA-256 dla całości dokumentu zakodowanego Base64URL obejmującego wszystkie trzy elementy, czyli nagłówek, zawartość i podpis dokumentu. Należy zaznaczyć iż nagłówek JWS zawiera wartość funkcji skrótu poprzedniego dokumentu o ile taki istniał.

Wyznaczanie skrótu dokumentów w postaci elektronicznej opisane jest w punkcie A.10.4.

4.4.5 Weryfikacja ciągłości łańcucha dokumentów

Badanie ciągłości łańcucha dokumentów oprócz podpisu bieżącego dokumentu wymaga wskazania poprzedniego dokumentu danego typu celem uzyskania jego skrótu SHA2. Dlatego wymagane jest umieszczenie w bieżącym dokumencie identyfikatora poprzedniego dokumentu, który składa się z osiemnastu cyfr, a jeśli jest to pierwszy dokument danego typu to z osiemnastu zer.

W celu określenia identyfikatora poprzedniego dokumentu należy połączyć znakowo identyfikator pamięci chronionej poprzedniego dokumentu "pamiecChr", który dla kas w postaci oprogramowania zawsze ma wartość równą jeden oraz identyfikatora dokumentu "JPKID" dopełniając

obie wartości zerami odpowiednio do trzech i do piętnastu miejsc tak aby wynik składał się z osiemnastu cyfr.

Mechanizm weryfikacji ciągłości łańcucha dokumentów opisany jest w punkcie A.10.5.

4.4.6 Tworzenie kodu weryfikującego dokument w postaci elektronicznej

Do utworzenia kodu weryfikującego dokument należy użyć bajtowo połączonych danych:

- wartość funkcji skrótu dokumentu,
- numer unikatowy kasy,
- numer kolejny dokumentu,
- znacznik czasu odzwierciedlający datę i czas zakończenia sprzedaży,
- kod autoryzacyjny.

Utworzenie kodu autoryzacyjnego opiera się na wykorzystaniu metody tworzenia kodu uwierzytelnienia wiadomości (MAC - Message Authentication Code) z wykorzystaniem funkcji skrótu (haszowania) SHA-256. Parametrami wejściowymi funkcji HMAC-256 jest tablica bajtowa utworzona z połączonych bajtowo wymienionych powyżej atrybutów: wartość funkcji skrótu SHA-256 dokumentu obliczona zgodnie z punktem 4.4.4 (32 bajty), numer unikatowy kasy tablica bajtowa znaków ASCI (13 bajtów), numer kolejny dokumentu (JPKID wraz z numerem pamięci chronionej) (8 bajtów), znacznik czasu odzwierciedlający datę i czas zakończenia sprzedaży w postaci numerycznej - UNIX timestamp w milisekundach (8 bajtów). Kluczem funkcji haszującej jest ważny na dzień wystawienia dokumentu klucz współdzielony pobrany z serwera CPD.

Utworzenie kodu weryfikującego polega na połączeniu bajtowym kolejno atrybutów: wartości funkcji skrótu SHA-256 dokumentu (32 bajty), numeru unikatowego kasy (13 bajtów), numeru kolejnego dokumentu (JPKID wraz z numerem pamięci chronionej) (8 bajtów), znacznika czasu w postaci numerycznej - UNIX timestamp w milisekundach (8 bajtów) oraz wyliczonego kodu autoryzacyjnego (32 bajty).

Szczegółowy opis usługi pobierania kluczy współdzielonych zawiera dokument „Opis techniczny protokołu komunikacyjnego kasa – Centralne Repozytorium Kas – Specyfikacja komend”.

Natomiast sposób weryfikacji kodu autoryzacyjnego na podstawie przesłanego kodu weryfikującego opisany jest w dokumencie „Centralne Repozytorium Kas – Opis usługi sprawdzającej kod weryfikujący paragonu”.

Szczegółowy opis mechanizmu tworzenia kodu przedstawiono w punkcie A.10.6.

5 Szyfrowanie komend oraz zbiorów danych i dokumentów w postaci elektronicznej

Wszystkie dane (dokumenty, komendy, odpowiedzi, raporty itp.) przechodzące przez publiczną chmurę są podpisywane i szyfrowane zarówno przez kasę fiskalną jak i serwer CPD. Klucz publiczny jest przesyłany w formie certyfikatu X.509 podpisanego przez wystawcę w formacie binarnym DER zakodowanym Base64 bez znacznika początku i końca certyfikatu oraz bez znaków końca linii. Kasa fiskalna powinna posiadać przyporządkowane dwie pary unikalnych kluczy asymetrycznych. Jedna z par kluczy wykorzystywana jest do dwustronnej komunikacji TLS z chmurą publiczną oraz serwerem CPD. Druga para kluczy wykorzystywana jest do podpisywania i szyfrowania wymienianych danych. Klucze prywatne przechowywane są w kasie fiskalnej. Klucz publiczny używany do szyfrowania danych powinien zostać przesłany do serwera CPD w celu weryfikacji wystawcy oraz późniejszego użycia do komunikacji z kasą. Przesłany klucz publiczny przyporządkowany jest dokładnie jednej kasie i przechowywany w zasobach ministerstwa.

Nazwy atrybutów kluczy kasy fiskalnej

Nazwa tagu	Opis
-digitalCertificateCashRegisterTLS	Certyfikat kasy do komunikacji TLS z serwerem CPD i chmurą Azure.
-privateKeyCashRegisterTLS	Klucz prywatny kasy do komunikacji TLS z serwerem CPD i chmurą Azure.
-digitalCertificateCashRegisterEncrypt	Certyfikat urządzenia fiskalnego do szyfrowania wymienianych danych
-privateKeyCashRegisterEncrypt	Klucz prywatny kasy do podpisywania wymienianych danych

Repozytorium operuje na trzech parach unikalnych kluczy:

- do dwustronnej komunikacji TLS kasy fiskalnej z serwerem CPD,
- do dwustronnej komunikacji TLS kasy z chmurą publiczną,
- do podpisywania i szyfrowania przesyłanych komend.

Klucze prywatne przechowywane są w zasobach ministerstwa, natomiast klucze publiczne repozytorium oraz klucz publiczny CA usługi przyjmowania danych chmury publicznej są przesyłane do kasy podczas procesu fiskalizacji w postaci certyfikatu X.509 podpisanego przez wystawcę w formacie binarnym DER zakodowanym Base64 bez znacznika początku i końca certyfikatu oraz bez znaków końca linii. Dodatkowo repozytorium przechowuje certyfikaty zaufanych producentów kas w celu weryfikacji kluczy publicznych kas fiskalnych.

Nazwy tagów kluczy Repozytorium

Nazwa tagu	Opis
-digitalCertificateWebApiTLS	Certyfikat WebAPI do komunikacji TLS z kasą fiskalną
-privateKeyWebApiTLS	Klucz prywatny WebAPI do komunikacji TLS z kasą fiskalną
-digitalCertificateCPDServerTLS	Certyfikat serwera CPD do komunikacji TLS z kasą fiskalną
-privateKeyCPDServerTLS	Klucz prywatny serwera CPD do komunikacji TLS z kasą fiskalną
-digitalCertificateRepositoryEncrypt	Certyfikat serwera CPD do szyfrowania komend przesyłanych do kasy
-privateKeyRepositoryEncrypt	Klucz prywatny serwera CPD do podpisywania komend przesyłanych do kasy
-digitalCertificateAzureEventHubTLS	Certyfikaty usługi EventHub na chmurze Azure do komunikacji TLS

5.1 Podpisywanie i szyfrowanie komend

Podpisywanie oraz szyfrowanie komend realizowane jest przez repozytorium z wykorzystaniem obiektów JWS oraz JWE struktury JSON w formacie JOSE z wykorzystaniem kodowania Base64URL. W pierwszej kolejności realizowany jest podpis, a następnie szyfrowanie podpisanej komendy.

Etapy przygotowania paczki:

- utworzenie obiektu JSON zgodnie z formatem danej komendy po przez wypełnienie pola "*attributes*" parametrami opisanymi w dokumencie „Opis techniczny protokołu komunikacyjnego kasa – Centralne Repozytorium Kas – Specyfikacja komend",

- utworzenie obiektu JWS - podpisanie obiektu JSON zawierającego pole "*attributes*" algorytmem RSA z dopełnieniem PKCS1-v1.5 i funkcją haszującą SHA-256 oraz dodanie parametrów nagłówka JOSE:

    - "*alg*" zawierającego symbol użytego algorytmu podpisu (RS256),
    - "*x5c*" zawierającego zgodnie z opisem w sekcji 4.1.6 dokumentu RFC 7515 jednoelementową tablicę JSON z certyfikatem podpisującym ministerstwa w formacie DER zakodowanym Base64 bez znacznika początku i końca certyfikatu oraz bez znaków końca linii,

- utworzenie obiektu JWE - zaszyfrowanie obiektu JWS algorytmem AES 128 CBC z uwierzytelnieniem wiadomości funkcją skrótu SHA-256 (AES_CBC_HMAC_SHA2) oraz klucza algorytmem RSA z dopełnieniem PKCS1-v1.5 oraz dodanie parametrów nagłówka JOSE:

    - "*alg*" zawierającego symbol użytego algorytmu podpisu (RSA1_5),
    - "*enc*" zawierającego symbol użytego algorytmu szyfrującego (A128CBC-HS256),
    - "*kid*" zawierającego numer seryjny oraz wystawcę certyfikatu klucza publicznego użytego do zaszyfrowania klucza szyfrującego,

- utworzenie paczki z polem "*commandId*" i "*encryptedCommand*" zawierającym obiekt JWE.

Szczegółowy opis podpisywania oraz szyfrowania zaprezentowany jest w załącznikach A.2 oraz A.3.

5.2 Podpisywanie i szyfrowanie zbiorów danych oraz dokumentów w postaci elektronicznej

Podpisywanie oraz szyfrowanie zbioru danych oraz dokumentów w postaci elektronicznej realizowane jest z wykorzystaniem obiektów JWS oraz JWE struktury JSON w formacie JOSE z wykorzystaniem kodowania Base64URL. W pierwszej kolejności realizowany jest podpis, a następnie szyfrowanie podpisanych danych.

Etapy przygotowania paczki:

- utworzenie obiektu JSON zgodnie z aktualnym schematem dokumentu JPK, dostępne następujące rodzaje schematów:
  - struktura zbioru danych dla kas rejestrujących,
  - struktura zbioru danych dla kas rejestrujących online,
  - struktura zbioru danych dla kas rejestrujących w postaci oprogramowania,
  - struktura dokumentu w postaci elektronicznej dla kas rejestrujących online,
  - struktura dokumentu w postaci elektronicznej dla kas rejestrujących w postaci oprogramowania,
- utworzenie obiektu JWS - podpisanie obiektu JSON lub skompresowanych danych algorytmem RSA z dopełnieniem PKCS1-v1.5 i funkcją haszującą SHA-256 oraz dodanie parametrów nagłówka JOSE:

  dla zbioru danych:

  - ”*alg*” zawierającego symbol użytego algorytmu podpisu (RS256),
  - ”*jpkmetadata*” zawierającego zakodowany w Base64 obiekt JSON składający się z opcjonalnych parametrów opisujących numer korelacyjny komendy oraz metodę kompresowania,
  - ”*jpkcertificate*” zawierający certyfikat klucza publicznego użyty do podpisu w formacie DER zakodowanym Base64 bez znacznika początku i końca certyfikatu oraz bez znaków końca linii,

  dla dokumentów w postaci elektronicznej:

  - ”*alg*” zawierającego symbol użytego algorytmu podpisu (RS256),
  - ”*jpkmetadata*” zawierającego zakodowany w Base64 obiekt JSON składający się z opcjonalnych parametrów opisujących numer korelacyjny komendy oraz metodę kompresowania,
  - ”*x5c*” zawierającego zgodnie z opisem w sekcji 4.1.6 dokumentu RFC 7515 jednoelementową tablicę JSON z certyfikatem klucza publicznego użytym do podpisu, w formacie DER zakodowanym Base64 bez znacznika początku i końca certyfikatu oraz bez znaków końca linii,
  - *”eParagon.mf.gov.pl”* zawierającego zakodowany w Base64 obiekt JSON składający się z parametrów: identyfikatora bieżącego dokumentu ”*JPKID*” (wraz z numerem pamięci chronionej), wersji schematu użytej struktury JSON ”*wersja*”, daty i czasu wystawienia dokumentu ”*dataJPK*” oraz elementu ”*JPKREF*” zawierającego identyfikator ”*JPKID*” (wraz z numerem pamięci chronionej) i wartość funkcji skrótu ”*SHA256*” poprzedniego dokumentu,

- utworzenie obiektu JWE - zaszyfrowanie obiektu JWS algorytmem AES 128 CBC z uwierzytelnieniem wiadomości funkcją skrótu SHA-256 (AES_CBC_HMAC_SHA2) oraz klucza algorytmem RSA z dopełnieniem PKCS1-v1.5 oraz dodanie parametrów nagłówka JOSE:
    - ”*alg*” zawierającego symbol użytego algorytmu podpisu (RSA1_5),
    - ”*enc*” zawierającego symbol użytego algorytmu szyfrującego (A128CBC-HS256),
    - ”*kid*” zawierającego numer seryjny oraz wystawcę certyfikatu klucza publicznego użytego do zaszyfrowania klucza szyfrującego,

- opcjonalnie podział danych na części nie większe niż 1 MB - limit usługi EventHub,

- utworzenie paczki/paczek z odpowiednimi wartościami atrybutów "*commandId*", "*packageNr*", "*isLast*" oraz polem "*encryptedData*" zawierającym cały obiekt JWE albo podzielone binarnie jego części.

Szczegółowy opis podpisywania oraz szyfrowania danych przedstawiono w załącznikach A.4 oraz A.5.

Załącznik A

A.1 Funkcje użyte w opisach

- UTF8 - funkcja zapisująca zbiór bajtów w łańcuch znaków w kodowaniu UTF8.
- SHA256 - funkcja skrótu używająca algorytmu SHA-256.
- BASE64 - funkcja kodująca dane zgodnie ze specyfikacją RFC 4648.
- DecodeB64 - funkcja dekodująca dane zgodnie ze specyfikacją RFC 4648.
- BASE64URL - funkcja kodująca dane zgodnie z załącznikiem C dokumentu RFC 7515.
- DecodeB64URL - funkcja dekodująca dane zgodnie z załącznikiem C dokumentu RFC 7515.
- RANDOM - funkcja generująca pseudolosowy ciąg bajtów - Strong Random Generator (RNG).
- DEFLATE - funkcja kompresująca dane algorytmem opisanym w dokumencie RFC 1951.
- INFLATE - funkcja dekompresująca dane algorytmem w dokumencie RFC 1951.
- RS256 - funkcja podpisująca algorytmem RSA z wykorzystaniem SHA-256.
- RS256Verify - funkcja weryfikująca podpis algorytmem RSA z wykorzystaniem SHA-256.
- HS256 - funkcja generująca MAC algorytmem SHA-256 zgodnie z RFC 2104, argumenty:
  - dodatkowe dane autoryzujące (AAD),
  - klucz haszujący.
- A128CBC – funkcja szyfrująca dane, argumenty to:
  - jawny tekst
  - klucz szyfrujący
  - wektor inicjujący (IV).
- A128CBCDecrypt – funkcja odszyfrowująca dane, argumenty to:
  - zaszyfrowany tekst
  - klucz szyfrujący
  - wektor inicjujący (IV).
- RSA1_5 - funkcja szyfrująca klucz symetryczny algorytmem RSA.
- RSA1_5Decrypt - funkcja odszyfrowująca klucz symetryczny algorytmem RSA.
- || - operator łączący dwa łańcuchy znaków (np. ‘Hello’ || ‘ world’ => ‘Hello world’).

A.2 Podpisywanie komend

Załącznik przedstawia sposób podpisywania komend wysyłanych z repozytorium do kasy fiskalnej, wzorowany na opisie zawartym w załączniku A.2 specyfikacji RFC 7515.

1. Przygotowanie chronionego nagłówka podpisu (JWS Protected Header):
   - wyszczególnienie użytego algorytmu podpisu w parametrze ”*alg*”,
   - dodanie parametru ”*x5c*” zawierającego jednoelementową tablicę z certyfikatem klucza publicznego ministerstwa użytego do podpisu w formacie DER zakodowanym Base64 bez znacznika początku i końca certyfikatu oraz bez znaków końca linii,
     UWAGA: ciąg znaków reprezentujący certyfikat może zostać poszerzony o wstawienie znaku specjalnego ‘\’ poprzedzającego znak ‘/’.

   Skrócona postać nagłówka w formacie JSON:

   ```
   JWS_PH => {"alg":"RS256","x5c":["MIIFHDCCAwSgAwIBAgITOgAA … 0NCJ2zprYt8XrNO728ljyA=="]}
   ```

   Pełna postać z wykorzystaniem certyfikatu testowego B.1.1 przedstawiona jest w punkcie B.2.1.

2. Przygotowany nagłówek przekształcany jest przez kodowanie Base64URL:

   ```
   JWS_PH_URL => BASE64URL(JWS_PH)
   ```

   Skrócona postać nagłówka w formacie Base64URL:

   ```
   JWS_PH_URL => eyJhbGciOiJSUzI1NiIsIng1 … 0OFhyTk83MjhsanlBPT0iXX0
   ```

   Pełna postać nagłówka zakodowanego Base64URL przedstawiona jest w punkcie B.2.2.

3. Przygotowanie zawartości komendy do podpisu:

   ```
   JWS_DATA => {"attributes":{"cpdServiceName":"KFD"}}
   ```

   W przykładzie użyto komendę CMD01 nakazującą kasie fiskalnej połączenie się z serwerem CPD i wywołanie wskazanej usługi (KFD – wykonanie komendy CMD08: Wyślij certyfikaty kasy fiskalnej).

4. Przygotowane dane należy zakodować w Base64URL:

   ```
   JWS_DATA_URL => BASE64URL(JWS_DATA)
   ```

   Postać przykładowych danych w formacie Base64URL:

   ```
   JWS_DATA_URL => eyJhdHRyaWJ1dGVzIjp7ImNwZFNlcnZpY2VOYW1lIjoiS0ZEIn19
   ```

   Pełna postać danych zakodowanego Base64URL przedstawiona jest w punkcie B.2.3.

5. Przygotowanie danych do popisu polegające na połączeniu nagłówka i danych zakodowanych w Base64URL rozdzielonych kropką:

   ```
   JWS_SIGNING_INPUT => JWS_PH_URL||.||JWS_DATA_URL
   ```

   Skrócona postać przykładowych danych do popisu w formacie Base64URL:

```
JWS_SIGNING_INPUT => eyJhbGciOiJSUzI1NiIsIng1 … cnZpY2VOYW1lIjoiS0ZEIn19
```

Pełna postać przykładowych danych do podpisu zakodowanych Base64URL przedstawiona jest w punkcie B.2.4.

Wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona na danych do podpisu z punktu B.2.4:

```
68e24de4af1da3859f0e8658b229f8aa01950d56cfa1bbf8c4cb3c55d49683e9
```

6. Tworzenie podpisu z wykorzystaniem algorytmu RSA z funkcja skrótu SHA-256 oraz klucza prywatnego ministerstwa i zakodowanie podpisu Base64URL:

```
JWS_SIGN => RS256(JWS_SIGNING_INPUT,RSA_PRIVATE_KEY)
```

Otrzymany podpis zapisywany jest w kodowaniu Base64URL:

```
JWS_SIGN_URL => BASE64URL(JWS_SIGN)
```

Skrócona postać podpisu w formacie Base64URL:

```
JWS_SIGN_URL => HlKhuau2-ZLYoBip8ed2J7Js … 8o7mxe-FFv1RLSP1zoMU-NGHw
```

Pełna postać przykładowego podpisu zakodowanego Base64URL przedstawiona jest w punkcie B.2.5.

7. Przygotowanie obiektu JWS polegające na połączeniu danych do podpisu i otrzymanego podpisu zakodowanych w Base64URL rozdzielonych kropką:

```
JWS => JWS_SIGNING_INPUT||.||JWS_SIGN_URL
```

```
albo
```

```
JWS => JWS_PH_URL||.||JWS_DATA_URL||.||JWS_SIGN_URL
```

Pełna postać przykładowego obiektu JWS z wykorzystaniem certyfikatu B.1.1 przedstawiona jest w punkcie B.2.6.

A.3 Szyfrowanie komend

Załącznik przedstawia sposób szyfrowania komend wysyłanych z repozytorium do kasy fiskalnej, wzorowany na opisie zawartym w załączniku A.2 specyfikacji RFC 7516.

1. Przygotowanie chronionego nagłówka szyfrowania (JWE Protected Header):
    - wyszczególnienie algorytmu asymetrycznego szyfrowania klucza w parametrze ”*alg*”,
    - wyszczególnienie algorytmu symetrycznego szyfrowania danych w parametrze ”*enc*”,
    - dodanie parametru ”*kid*” zawierającego numer seryjny w postaci szesnastkowej oraz nazwę wystawcy „common name” certyfikatu klucza publicznego użytego do zaszyfrowania klucza szyfrującego.

    Przykładowa postać nagłówka w formacie JSON:

    ```
    JWE_PH => {"enc":"A128CBC-HS256","alg":"RSA1_5","kid":"0A2B4C6D8E0F,CN=Producent"}
    ```

    Pełna postać z wykorzystaniem certyfikatu testowego B.1.2 przedstawiona jest w punkcie B.3.1.

2. Przygotowany nagłówek przekształcany jest przez kodowanie Base64URL:

    ```
    JWE_PH_URL => BASE64URL(JWE_PH)
    ```

    Pełna postać nagłówka zakodowanego Base64URL przedstawiona jest w punkcie B.3.2.

3. Przygotowanie danych używanych do szyfrowania symetrycznego:
    - wygenerowanie 32 bajtowego losowego klucza algorytmu szyfrującego,
    - wydzielenie pierwszych 16 bajtów klucza algorytmu szyfrującego jako klucz haszujący,
    - wydzielenie ostatnich 16 bajtów klucza algorytmu szyfrującego jako klucz szyfrujący,
    - wygenerowanie 16 bajtowego losowego wektora inicjującego,

    ```
    JWE_AES_CEK => RANDOM(32)

    JWE_MAC_KEY => FIRST 16 BYTES FROM JWE_AES_CEK
    JWE_AES_KEY => LAST 16 BYTES FROM JWE_AES_CEK

    JWE_AES_IV => RANDOM(16)
    ```

    Wartości zastosowane w przykładach przedstawiono w punkcie B.3.3.

4. Zaszyfrowanie klucza algorytmu szyfrującego (Content Encryption Key) składającego się z klucza haszującego i klucza szyfrującego z wykorzystaniem algorytmu asymetrycznego RSA kluczem publicznym kasy fiskalnej i zakodowanie w Base64URL:

    ```
    JWE_CEK_URL => BASE64URL(RSA1_5(JWE_AES_CEK,RSA_PUBLIC_KEY))
    ```

    Przykładowa wartość zakodowana w Base64URL z użyciem certyfikatu B.1.2 przedstawiona jest w punkcie B.3.4.

5. Zakodowanie wektora inicjującego w Base64URL:

    ```
    JWE_IV_URL => BASE64URL(JWE_AES_IV)
    ```

    Przykładowa wartość zakodowanego wektora inicjującego w Base64URL przedstawiona jest w punkcie B.3.5.

6. Zaszyfrowanie podpisanej komendy algorytmem symetrycznym:

```
JWE_TXT_URL => BASE64URL(A128CBC(JWS,JWE_AES_KEY,JWE_AES_IV))
```

Przykładowa wartość zakodowanego Base64URL przedstawiona jest w punkcie B.3.6.

7. Przygotowanie dodatkowych danych uwierzytelniających (Additional Authenticated Data) poprzez użycie utworzonego chronionego nagłówka szyfrowania (JWE Protected Header):

```
JWE_AAD_URL => JWE_PH_URL
```

Przykładową wartość dodatkowych danych uwierzytelniających w postaci Base64URL przedstawiono w punkcie B.3.7a.

Obliczenie AL (ADD Length) - liczby bitów dodatkowych danych uwierzytelniających (AAD) oraz przedstawienie tej wartości w postaci 64-bitowej liczby w formacie Big-Endian.

```
JWE_AL => JWE_AAD_URL BITS LENGTH CONVERT TO 64 BIT BIG-ENDIAN VALUE
```

Przykład utworzenia tablicy bajtów odzwierciedlającej długość ADD przedstawiony jest w punkcie B.3.7b.

8. Wyliczenie etykiety uwierzytelniającej (Authentication Tag) z wykorzystaniem funkcji HMAC z funkcją haszującą SHA-256 przy użyciu klucza haszującego i połączonych tablic bajtów dodatkowych danych uwierzytelniających (AAD), wektora inicjującego (IV), zaszyfrowanych danych oraz wektora długości AAD (AL) i użycie pierwszych 16 bajtów wyliczonej wartości:

```
JWE_AT_DATA => JWE_AAD_URL_BYTES||JWE_AES_IV||DecodeB64URL(JWE_TXT_URL)||JWE_AL

JWE_AT_256 => HS256(JWE_AT_DATA, JWE_MAC_KEY)

JWE_AT => FIRST 16 BYTES FROM JWE_AT_256
```

Przykładowa wartość przedstawiona jest w punkcie B.3.8a, a sposób wyliczenia w punkcie B.3.8b.

9. Przygotowanie obiektu JWE polegające na połączeniu chronionego nagłówka szyfrowania (JWE Protected Header), zaszyfrowanego klucza algorytmu szyfrującego (CEK), wektora inicjującego (IV), zaszyfrowanych danych oraz etykiety uwierzytelniającej (Authentication Tag) rozdzielonych kropką:

```
JWE => JWE_PH_URL||'.'||JWE_CEK_URL||'.'||JWE_IV_URL||'.'||JWE_TXT_URL||'.'||JWE_AT_URL
```

Przykładowa wartość zakodowanego Base64URL przedstawiona jest w punkcie B.3.9.

A.4 Podpisywanie danych

Załącznik przedstawia sposób podpisywania danych wysyłanych z kasy fiskalnej do repozytorium, wzorowany na opisie zawartym w załączniku A.2 specyfikacji RFC 7515.

1. Przygotowanie chronionego nagłówka podpisu (JWS Protected Header):
   - wyszczególnienie użytego algorytmu podpisu w parametrze ”*alg*”,
   - dodanie parametru ”*jpkcertificate*” zawierającego certyfikat klucza publicznego użytego do podpisu w formacie DER zakodowanym Base64 bez znacznika początku i końca certyfikatu oraz bez znaków końca linii,

   UWAGA: ciąg znaków reprezentujący certyfikat może zostać poszerzony o wstawienie znaku specjalnego ‘\’ poprzedzającego znak ‘/’,
   - dodanie opcjonalnego parametru ”*jpkmetadata*” zawierającego zakodowany w Base64 obiekt JSON składający się z opcjonalnych parametrów:
     - correlationId - numer korelacyjny, czyli identyfikator ”*commandId*” wykonywanej komendy pobranej z usługi WebApi, na przykład identyfikator harmonogramu przesyłania danych (TFD),
     - compression - metoda kompresowania przesyłanych danych:
       - DEFLATE - kompresja algorytmem opisanym w dokumencie RFC 1951,
       - NONE – przesłanie nieskompresowanych danych,
       - brak parametru ”compression” oznacza brak kompresji danych.

   UWAGA: ciąg znaków reprezentujący metadane może zostać poszerzony o wstawienie znaku specjalnego ‘\’ poprzedzającego znak ‘/’.

   Skrócona postać nagłówka w formacie JSON:

   ```
   JWS_PH => {"jpkcertificate":"MIIC … hZiS","alg":"RS256","jpkmetadata":"eyJj … In0="}
   ```

   Pełna postać z wykorzystaniem certyfikatu testowego przedstawiona jest w punkcie B.4.1.

   Przykładowa postać parametru ”*jpkmetadata*” w formacie JSON:

   ```
   {"correlationId":"TFD.ZTE1234567890.2018-01-01T01:00:00.000Z"}
   ```

   ```
   {"correlationId":"TFD.ZTE1234567890.2018-01-01T01:00:00.000Z","compression":"DEFLATE"}
   ```

2. Przygotowany nagłówek przekształcany jest przez kodowanie Base64URL:

   ```
   JWS_PH_URL => BASE64URL(JWS_PH)
   ```

   Pełna postać nagłówka zakodowanego Base64URL przedstawiona jest w punkcie B.4.2.

3. Przygotowanie zawartości danych do podpisu i opcjonalnie skompresowanie:

   ```
   JWS_DATA => { "JPK": { "naglowek": {…}, "podmiot1": {…}, "content": [ … ] } }
   ```

   ```
   opcjonalnie skompresowanie:
   ```

   ```
   JWS_DATA => DEFLATE(JWS_DATA)
   ```

   Pełna postać przykładowych nieskompresowanych danych przedstawiona jest w punkcie B.4.3.

4. Przygotowane dane należy zakodować w Base64URL:

   ```
   JWS_DATA_URL => BASE64URL(JWS_DATA)
   ```

   Pełna postać przykładowych danych zakodowanych Base64URL przedstawiona jest w punkcie B.4.4.

5. Przygotowanie zawartości do popisu polegające na połączeniu nagłówka i danych zakodowanych w Base64URL rozdzielonych kropką:

   ```
   JWS_SIGNING_INPUT => JWS_PH_URL||.||JWS_DATA_URL
   ```

6. Tworzenie podpisu z wykorzystaniem algorytmu RSA oraz klucza prywatnego kasy i zakodowanie podpisu Base64URL:

   ```
   JWS_SIGN_URL => BASE64URL(RS256(JWS_SIGNING_INPUT,RSA_PRIVATE_KEY))
   ```

7. Przygotowanie obiektu JWS polegające na połączeniu danych do podpisu i otrzymanego podpisu zakodowanych w Base64URL rozdzielonych kropką:

   ```
   JWS => JWS_SIGNING_INPUT||.||JWS_SIGN_URL
   ```

   albo

   ```
   JWS => JWS_PH_URL||.||JWS_DATA_URL||.||JWS_SIGN_URL
   ```

   Pełna postać przykładowego obiektu JWS z wykorzystaniem certyfikatu B.1.2 przedstawiona jest w punkcie B.4.5.

A.5 Szyfrowanie danych

Załącznik przedstawia sposób szyfrowania danych wysyłanych z kasy fiskalnej do repozytorium, wzorowany na opisie zawartym w załączniku A.2 specyfikacji RFC 7516.

1. Przygotowanie chronionego nagłówka szyfrowania (JWE Protected Header):
    - wyszczególnienie algorytmu asymetrycznego szyfrowania klucza w parametrze "*alg*",
    - wyszczególnienie algorytmu symetrycznego szyfrowania danych w parametrze "*enc*",
    - dodanie parametru "*kid*" zawierającego numer seryjny w postaci szesnastkowej oraz nazwę „common name" wystawcy certyfikatu klucza publicznego użytego do zaszyfrowania klucza szyfrującego.

    Przykładowa postać nagłówka w formacie JSON:

    ```
    JWE_PH => {"enc":"A128CBC-HS256","alg":"RSA1_5","kid":"0A2B4C6D8E0F, CN=Ministerstwo"}
    ```

    Pełna postać z wykorzystaniem certyfikatu testowego B.1.1 przedstawiona jest w punkcie B.5.1.

2. Przygotowany nagłówek przekształcany jest przez kodowanie Base64URL:

    ```
    JWE_PH_URL => BASE64URL(JWE_PH)
    ```

    Pełna postać nagłówka zakodowanego Base64URL przedstawiona jest w punkcie B.5.2.

3. Przygotowanie danych używanych do szyfrowania symetrycznego:
    - wygenerowanie 32 bajtowego losowego klucza algorytmu szyfrującego,
    - wydzielenie pierwszych 16 bajtów klucza algorytmu szyfrującego jako klucz haszujący,
    - wydzielenie ostatnich 16 bajtów klucza algorytmu szyfrującego jako klucz szyfrujący,
    - wygenerowanie 16 bajtowego losowego wektora inicjującego,

    ```
    JWE_AES_CEK => RANDOM(32)

    JWE_MAC_KEY => FIRST 16 BYTES FROM JWE_AES_CEK
    JWE_AES_KEY => LAST 16 BYTES FROM JWE_AES_CEK

    JWE_AES_IV => RANDOM(16)
    ```

    Wartości zastosowane w przykładach przedstawiono w punkcie B.5.3.

4. Zaszyfrowanie klucza algorytmu szyfrującego (Content Encryption Key) składającego się klucza haszującego i klucza szyfrującego z wykorzystaniem algorytmu asymetrycznego RSA kluczem publicznym ministerstwa i zakodowanie w Base64URL:

    ```
    JWE_CEK_URL => BASE64URL(RSA1_5(JWE_AES_CEK,RSA_PUBLIC_KEY))
    ```

    Przykładowa wartość zakodowana w Base64URL z użyciem certyfikatu B.1.1 przedstawiona jest w punkcie B.5.4.

5. Zakodowanie wektora inicjującego (IV) w Base64URL:

    ```
    JWE_IV_URL => BASE64URL(JWE_AES_IV)
    ```

    Przykładowa wartość zakodowanego wektora inicjującego w Base64URL przedstawiona jest w punkcie B.5.5.

6. Zaszyfrowanie podpisanej komendy algorytmem symetrycznym:

```
JWE_TXT_URL => BASE64URL(A128CBC(JWS,JWE_AES_KEY,JWE_AES_IV))
```

Przykładowa wartość zakodowanego Base64URL przedstawiona jest w punkcie B.5.6.

7. Przygotowanie dodatkowych danych uwierzytelniających (Additional Authenticated Data) poprzez użycie utworzonego chronionego nagłówka szyfrowania (JWE Protected Header):

```
JWE_AAD_URL => JWE_PH_URL
```

Przykładowa wartość przedstawiona jest w punkcie B.5.7a.

Obliczenie AL (ADD Length) - liczby bitów dodatkowych danych uwierzytelniających (AAD) oraz przedstawienie tej wartości w postaci 64-bitowej liczby w formacie Big-Endian.

```
JWE_AL => JWE_AAD_URL BITS LENGTH CONVERT TO 64 BIT BIG-ENDIAN VALUE
```

Przykładowa wartość zakodowanego Base64URL przedstawiona jest w punkcie B.5.7b.

8. Wyliczenie etykiety uwierzytelniającej (Authentication Tag) z wykorzystaniem funkcji HMAC z funkcją haszującą SHA-256 przy użyciu klucza haszującego i połączonych tablic bajtów dodatkowych danych uwierzytelniających (AAD), wektora inicjującego (IV), zaszyfrowanych danych oraz wektora długości AAD (AL) i użycie pierwszych 16 bajtów wyliczonej wartości:

```
JWE_AT_DATA => JWE_AAD_URL_BYTES||JWE_AES_IV||DecodeB64URL(JWE_TXT_URL)||JWE_AL

JWE_AT_256 => HS256(JWE_AT_DATA, JWE_MAC_KEY)

JWE_AT => FIRST 16 BYTES FROM JWE_AT_256
```

Przykładowa wartość przedstawiona jest w punkcie B.5.8a, a sposób wyliczenia w punkcie B.5.8b.

9. Przygotowanie obiektu JWE polegające na połączeniu chronionego nagłówka szyfrowania (JWE Protected Header), zaszyfrowanego klucza algorytmu szyfrującego (CEK), wektora inicjującego (IV), zaszyfrowanych danych oraz etykiety uwierzytelniającej (Authentication Tag) rozdzielonych kropką:

```
JWE => JWE_PH_URL||'.'||JWE_CEK_URL||'.'||JWE_IV_URL||'.'||JWE_TXT_URL||'.'||JWE_AT_URL
```

Przykładowa wartość zakodowanego Base64URL przedstawiona jest w punkcie B.5.9.

A.6 Wysyłanie danych

Przygotowanie paczki zawierającej podpisane i zaszyfrowane dane polega na wygenerowaniu identyfikatora paczki w formacie opisanym w dokumencie „Opis techniczny protokołu komunikacyjnego kasa – Centralne Repozytorium Kas – Specyfikacja komend” i umieszczenie otrzymanej wartości w parametrze "*commandId*". Natomiast zaszyfrowane dane należy umieścić w parametrze "*encryptedData*". Jeżeli rozmiar tworzonej paczki przekracza wielkość 1 MB to należy utworzyć z tym samym identyfikatorem kilka paczek nie przekraczających wskazany limit (cała paczka wraz z parametrami nie może przekraczać maksymalnej wielkości). Kolejny numer paczki należy zamieścić w parametrze "*packageNr*", aczkolwiek dla pojedynczej paczki musi on mieć wartość równą zero. Parametrem wymaganym do scalenia dokumentu jest parametr "*isLast*", którego wartość równa jeden określa ostatnią paczkę w przeciwnym wypadku powinien mieć wartość zero. Poszczególne paczki z uzyskanymi w wyniku podziału fragmentami należy przesłać jako osobny komunikat do usługi EventHub chmury Azure.

Przykład dla dokumentu składającego się tylko z jednego fragmentu:

```
{ "commandId": "DFD.AAA1234567890.2017-07-01T00:00:00.000Z", "packageNr": 0, "isLast":1,
"encryptedData": JWE }
```

Przykład dla dokumentu składającego się z wielu fragmentów:

```
JWE1||JWE2||JWE3 => JWE

{ "commandId": "DFD.AAA1234567890.2017-07-01T00:00:00.000Z", "packageNr": 1, "isLast":0,
"encryptedData": JWE1 }

{ "commandId": "DFD.AAA1234567890.2017-07-01T00:00:00.000Z", "packageNr": 2, "isLast":0,
"encryptedData": JWE2 }

{ "commandId": "DFD.AAA1234567890.2017-07-01T00:00:00.000Z", "packageNr": 3, "isLast":1,
"encryptedData": JWE3 }
```

A.7 Odebranie komendy

Po poprawnym zakończeniu procesu fiskalizacji opisanym w dokumencie „Opis techniczny protokołu komunikacyjnego kasa – Centralne Repozytorium Kas – Specyfikacja komend” opierającym się na komunikacji z serwerem CPD kasa przełącza się na komunikację z usługą WebApi umieszczoną w publicznej chmurze Azure. Kasa fiskalna komunikując się z WebApi pobiera przygotowane w formacie JSON paczki zawierające podpisane i zaszyfrowane komendy. Każda paczka zawiera w parametrze "*commandId*" wygenerowany identyfikator komendy w formacie opisanym w dokumencie „Opis techniczny protokołu komunikacyjnego kasa – Centralne Repozytorium Kas – Specyfikacja komend” oraz podpisaną i zaszyfrowaną komendę w parametrze "*encryptedCommand*".

Przykład komendy składającego się tylko z jednego fragmentu:

```
{ "commandId": "CCS.ZTE1701000901.2018-03-30T09:56:29.062Z", "encryptedCommand": JWE }
```

A.8 Odszyfrowanie komendy

Odebrana komenda ma format obiektu JWE składającego się z rozdzielonych kropką członów - chronionego nagłówka szyfrowania (JWE Protected Header), zaszyfrowanego klucza algorytmu szyfrującego (CEK), wektora inicjującego (IV), zaszyfrowanych danych oraz etykiety uwierzytelniającej (Authentication Tag):

```
JWE_PH_URL||'.'||JWE_CEK_URL||'.'||JWE_IV_URL||'.'||JWE_TXT_URL||'.'||JWE_AT_URL => JWE
```

Wyodrębnienie poszczególnych części pozwoli na poprawne zweryfikowanie i odszyfrowanie pobranej komendy.

1. Odkodowanie Base64URL chronionego nagłówka szyfrowania (JWE Protected Header) pozwoli na pobranie informacji o zastosowanych algorytmach szyfrowania (parametry „*enc*" oraz „*alg*") oraz zidentyfikowaniu użytego certyfikatu (parametr „*kid*").

   ```
   JWE_PH => DecodeB64URL(JWE_PH_URL)
   ```

2. Następnie należy odszyfrować klucz przy użyciu klucza prywatnego kasy, a z otrzymanej 32 bajtowej wartości wydzielić 16 bajtowy klucz haszujący oraz 16 bajtowy klucz szyfrujący:

   ```
   JWE_AES_CEK => RSA1_5Decrypt(DecodeB64URL(JWE_CEK_URL),RSA_PRIVATE_KEY)

   JWE_MAC_KEY => FIRST 16 BYTES FROM JWE_AES_CEK
   JWE_AES_KEY => LAST 16 BYTES FROM JWE_AES_CEK
   ```

3. Odkodowanie Base64URL wektora inicjującego:

   ```
   JWE_AES_IV => DecodeB64URL(JWE_IV_URL)
   ```

4. Przygotowanie dodatkowych danych uwierzytelniających (Additional Authenticated Data) poprzez użycie wyodrębnionego chronionego nagłówka szyfrowania (JWE Protected Header):

   ```
   JWE_AAD_URL => JWE_PH_URL
   ```

   Obliczenie AL (ADD Length) - liczby bitów dodatkowych danych uwierzytelniających (AAD) oraz przedstawienie tej wartości w postaci 64-bitowej liczby w formacie Big-Endian.

   ```
   JWE_AL => JWE_AAD_URL BITS LENGTH CONVERT TO 64 BIT BIG-ENDIAN VALUE
   ```

5. Wyliczenie etykiety uwierzytelniającej (Authentication Tag) z wykorzystaniem funkcji HMAC z funkcją haszującą SHA-256 przy użyciu odszyfrowanego klucza haszującego i połączonych tablic bajtów wyodrębnionych części - dodatkowych danych uwierzytelniających (AAD), wektora inicjującego (IV), zaszyfrowanych danych oraz wektora długości AAD (AL) oraz porównanie pierwszych 16 bajtów wyliczonej wartości z odebraną etykietą uwierzytelniającą (AT):

   ```
   JWE_AT_DATA => JWE_AAD_URL_BYTES||JWE_AES_IV||DecodeB64URL(JWE_TXT_URL)||JWE_AL

   JWE_AT_256 => HS256(JWE_AT_DATA, JWE_MAC_KEY)

   JWE_AT => FIRST 16 BYTES FROM JWE_AT_256
   ```

Pozytywny wynik porównania odebranej i wyliczonej etykiety uwierzytelniającej zapewnia kasie operowanie na wiarygodnych i integralnych danych.

Przykład wyliczenia etykiety uwierzytelniającej przedstawiony jest w punkcie B.3.8b.

10. Odszyfrowanie komendy algorytmem symetrycznym:

```
JWS => A128CBCDecrypt(DecodeB64URL(JWE_TXT_URL),JWE_AES_KEY,JWE_AES_IV)
```

W wyniku poprawnego odszyfrowania danych uzyskany zostanie obiekt JWS, czyli podpisana kluczem publicznym ministerstwa komenda.

A.9 Weryfikacja podpisu komendy

Odszyfrowana komenda ma format obiektu JWS składającego się z rozdzielonych kropką członów - chronionego nagłówka podpisu (JWS Protected Header), zakodowanych danych oraz podpisu:

```
JWS_PH_URL||.||JWS_DATA_URL||.||JWS_SIGN_URL => JWS
```

Weryfikowanie podpisu komendy:

1. Przygotowanie danych do weryfikacji popisu polegające na połączeniu nagłówka i danych zakodowanych w Base64URL rozdzielonych kropką:

   ```
   JWS_SIGNING_INPUT => JWS_PH_URL||.||JWS_DATA_URL
   ```

2. Odkodowanie chronionego nagłówka podpisu (JWS Protected Header) oraz pobranie informacji o zastosowanym algorytmie podpisu (parametr „*alg*”) i użytego certyfikatu (parametr „*x5c*”):

   ```
   JWS_PH => DecodeB64URL(JWS_PH_URL)
   ```

3. Weryfikacja przesłanego podpisu komendy z wykorzystaniem algorytmu asymetrycznego oraz klucza publicznego ministerstwa pobranego z parametru „*x5c*” chronionego nagłówka podpisu:

   ```
   RS256Verify(JWS_SIGNING_INPUT,JWS_SIGN,RSA_PUBLIC_KEY)
   ```

4. Weryfikacja certyfikatu klucza publicznego ministerstwa pobranego z nagłówka chronionego z certyfikatem pobranym w trakcie procesy fiskalizacji kasy.

A.10 Algorytmy kryptograficzne w kasach rejestrujących w postaci oprogramowania oraz kasach rejestrujących online

A.10.1 Podpisywanie dokumentów przesyłanych do repozytorium w zbiorach danych:

Poniżej przedstawiono sposób podpisywania poszczególnych dokumentów przesyłanych w zbiorach danych. W zależności od typu dokumentu wyszczególniono zestaw pól struktury JSON użytych do obliczenia wartości skrótu SHA2 funkcją SHA-256 i podpisaniem algorytmem RSA.

A.10.1a Podpisywanie raportu fiskalnego fiskalizacji:

1. Przygotowanie danych do podpisu polegające na połączeniu wyspecyfikowanych danych pobranych ze struktury JSON w jeden łańcuch:

   ```
   RAPFISK_SIGNING_INPUT => NIP||nrUnik||dataFisk||sumaZm||serwID
   ```

   Skrócona postać przykładowych danych do podpisu oparta na przykładzie z punktu C.2.1a:

   ```
   NIP       = 6970000802
   nrUnik    = WTE2001000009
   dataFisk  = 2020-04-10T01:23:45.678Z
   sumaZm    = 9DD845A0C9C285DC2E13F3253352E1836DC603C0
   serwID    = KW123

   RAPFISK_SIGNING_INPUT => 6970 … 10T01 … W123
   ```

   Pełna postać przykładowych danych do podpisu przedstawiona jest w punkcie C.2.3a.

   Wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona dla pełnych danych do podpisu dokumentu:

   ```
   fef1e767b2d728cf6ce5fc00f83ccc7be82748a86b1b7be59ec67b3bf1aa39c7
   ```

2. Tworzenie podpisu z wykorzystaniem algorytmu RSA z funkcją skrótu SHA-256 oraz klucza prywatnego kasy fisklanej:

   ```
   RAPFISK_SIGN => RS256(RAPFISK_SIGNING_INPUT,RSA_PRIVATE_KEY)
   ```

   Otrzymany podpis zapisywany jest w postaci szesnastkowej:

   ```
   RAPFISK_SIGN_HEX => HEX(RAPFISK_SIGN)
   ```

   Skrócona postać podpisu w postaci szesnastkowej:

   ```
   RAPFISK_SIGN_HEX => 3019505879124143c … 11fe22a622de55bb
   ```

   Pełna postać przykładowego podpisu w postaci szesnastkowej przedstawiona jest w punkcie C.2.4a.

   Pełną postać podpisu w postaci szesnastkowej należy zapisać w strukturze JSON w polu "RSA":

   ```
   rapFisk/podpis/RSA => RAPFISK_SIGN_HEX
   ```

A.10.1b Podpisywanie raportu fiskalnego dobowego:

1. Przygotowanie danych do podpisu polegające na połączeniu wyspecyfikowanych danych pobranych ze struktury JSON w jeden łańcuch:

   ```
   RAPDOB_SIGNING_INPUT => NIP||nrUnik||sprzedBrutto||podatekNal||zakRap
   ```

   Skrócona postać przykładowych danych do podpisu oparta na przykładzie z punktu C.2.1a:

   ```
   NIP          = 6970000802
   nrUnik       = WTE2001000009
   sprzedBrutto = 49060
   podatekNal   = 5060
   zakRap       = 2020-04-10T23:23:45.678Z

   RAPDOB_SIGNING_INPUT => 6970 … 10T23 … 678Z
   ```

   Pełna postać przykładowych danych do podpisu przedstawiona jest w punkcie C.2.3b.

   Wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona dla pełnych danych do podpisu dokumentu:

   ```
   6629368888063bbcc9cf80349d1a2b33b8d20f3ee6a0b4aabf15f51bc53d976e
   ```

2. Tworzenie podpisu z wykorzystaniem algorytmu RSA z funkcją skrótu SHA-256 oraz klucza prywatnego kasy fisklanej:

   ```
   RAPDOB_SIGN => RS256(RAPDOB_SIGNING_INPUT,RSA_PRIVATE_KEY)
   ```

   Otrzymany podpis zapisywany jest w postaci szesnastkowej:

   ```
   RAPDOB_SIGN_HEX => HEX(RAPDOB_SIGN)
   ```

   Skrócona postać podpisu w postaci szesnastkowej:

   ```
   RAPDOB_SIGN_HEX => 21184e6e94b7c822 … b8a257d9467f4c1ce
   ```

   Pełna postać przykładowego podpisu w postaci szesnastkowej przedstawiona jest w punkcie C.2.4b.

   Pełną postać podpisu w postaci szesnastkowej należy zapisać w strukturze JSON w polu "RSA":

   ```
   rapDob/podpis/RSA => RAPDOB_SIGN_HEX
   ```

A.10.1c Podpisywanie dokumentu niefiskalnego:

1. Przygotowanie danych do podpisu polegające na połączeniu wyspecyfikowanych danych pobranych ze struktury JSON w jeden łańcuch:

   ```
   NIEFISK_SIGNING_INPUT => NIP||nrUnik||nrDok||zak
   ```

   Skrócona postać przykładowych danych do podpisu oparta na przykładzie z punktu C.2.1a:

   ```
   NIP    = 6970000802
   nrUnik = WTE2001000009
   ```

```
nrDok  = 2
zak    = 2020-04-10T03:23:45.678Z

NIEFISK_SIGNING_INPUT => 6970 … 10T03 … 678Z
```

Pełna postać przykładowych danych do podpisu przedstawiona jest w punkcie C.2.3c.

Wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona dla pełnych danych do podpisu dokumentu:

```
1b46eb0df68a6a72766885366ef68ea42548491fc2608a75d8aedfa4cc720f6a
```

2. Tworzenie podpisu z wykorzystaniem algorytmu RSA z funkcją skrótu SHA-256 oraz klucza prywatnego kasy fiskalnej:

```
NIEFISK_SIGN => RS256(NIEFISK_SIGNING_INPUT,RSA_PRIVATE_KEY)
```

Otrzymany podpis zapisywany jest w postaci szesnastkowej:

```
NIEFISK_SIGN_HEX => HEX(NIEFISK_SIGN)
```

Skrócona postać podpisu w postaci szesnastkowej:

```
NIEFISK_SIGN_HEX => 282f2b77102bbb60 … fc5e1cbba9c79fb1
```

Pełna postać przykładowego podpisu w postaci szesnastkowej przedstawiona jest w punkcie C.2.4c.

Pełną postać podpisu w postaci szesnastkowej należy zapisać w strukturze JSON w polu "RSA":

```
wydrNiefisk/podpis/RSA => NIEFISK_SIGN_HEX
```

A.10.1d Podpisywanie paragonu anulowanego:

1. Przygotowanie danych do podpisu polegające na połączeniu wyspecyfikowanych danych pobranych ze struktury JSON w jeden łańcuch:

```
PARAGANUL_SIGNING_INPUT => NIP||nrUnik||nrDok||sumaBrutto||zakSprzed
```

Skrócona postać przykładowych danych do podpisu oparta na przykładzie z punktu C.2.1a:

```
NIP        = 6970000802
nrUnik     = WTE2001000009
nrDok      = 5
sumaBrutto = 1000000
zakSprzed  = 2020-04-10T06:23:45.678Z

PARAGANUL_SIGNING_INPUT => 6970 … 10T06 … 678Z
```

Pełna postać przykładowych danych do podpisu przedstawiona jest w punkcie C.2.3d.

Wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona dla pełnych danych do podpisu dokumentu:

```
9ebecd28bdcc0166b0967d67e048c1943a673215f014ce71e9424c0e82451e0f
```

2. Tworzenie podpisu z wykorzystaniem algorytmu RSA z funkcją skrótu SHA-256 oraz klucza prywatnego kasy fiskalnej:

```
PARAGANUL_SIGN => RS256(PARAGANUL_SIGNING_INPUT,RSA_PRIVATE_KEY)
```

Otrzymany podpis zapisywany jest w postaci szesnastkowej:

```
PARAGANUL_SIGN_HEX => HEX(PARAGANUL_SIGN)
```

Skrócona postać podpisu w postaci szesnastkowej:

```
PARAGANUL_SIGN_HEX => 9e61a538a24334c0 … 03e51453caa1c8f3
```

Pełna postać przykładowego podpisu w postaci szesnastkowej przedstawiona jest w punkcie C.2.4d.

Pełną postać podpisu w postaci szesnastkowej należy zapisać w strukturze JSON w polu "RSA":

```
paragAnul/podpis/RSA => PARAGANUL_SIGN_HEX
```

A.10.1e Podpisywanie faktury wyłącznie w kasach rejestrujących online:

1. Przygotowanie danych do podpisu polegające na połączeniu wyspecyfikowanych danych pobranych ze struktury JSON w jeden łańcuch:

```
FAKTURA_SIGNING_INPUT => NIP||nrUnik||nrDok||sumaBrutto||zakSprzed
```

Skrócona postać przykładowych danych do podpisu:

```
NIP        = 6970000802
nrUnik     = WTE2001000009
nrDok      = 5
sumaBrutto = 1000000
zakSprzed  = 2020-04-10T06:23:45.678Z

FAKTURA_SIGNING_INPUT => 6970 … 10T06 … 678Z
```

2. Tworzenie podpisu z wykorzystaniem algorytmu RSA z funkcją skrótu SHA-256 oraz klucza prywatnego kasy fiskalnej:

```
FAKTURA_SIGN => RS256(FAKTURA_SIGNING_INPUT,RSA_PRIVATE_KEY)
```

Otrzymany podpis zapisywany jest w postaci szesnastkowej:

```
FAKTURA_SIGN_HEX => HEX(FAKTURA_SIGN)
```

Skrócona postać podpisu w postaci szesnastkowej:

```
FAKTURA_SIGN_HEX => 9e61a538a24334c0 … 03e51453caa1c8f3
```

Pełną postać podpisu w postaci szesnastkowej należy zapisać w strukturze JSON w polu "RSA":

```
faktura/podpis/RSA => FAKTURA_SIGN_HEX
```

A.10.1f Podpisywanie faktury anulowanej wyłącznie w kasach rejestrujących online:

1. Przygotowanie danych do podpisu polegające na połączeniu wyspecyfikowanych danych pobranych ze struktury JSON w jeden łańcuch:

   ```
   FAANUL_SIGNING_INPUT => NIP||nrUnik||nrDok||sumaBrutto||zakSprzed
   ```

   Skrócona postać przykładowych danych do podpisu:

   ```
   NIP        = 6970000802
   nrUnik     = WTE2001000009
   nrDok      = 5
   sumaBrutto = 1000000
   zakSprzed  = 2020-04-10T06:23:45.678Z

   FAANUL_SIGNING_INPUT => 6970 … 10T06 … 678Z
   ```

2. Tworzenie podpisu z wykorzystaniem algorytmu RSA z funkcją skrótu SHA-256 oraz klucza prywatnego kasy fiskalnej:

   ```
   FAANUL_SIGN => RS256(FAANUL_SIGNING_INPUT,RSA_PRIVATE_KEY)
   ```

   Otrzymany podpis zapisywany jest w postaci szesnastkowej:

   ```
   FAANUL_SIGN_HEX => HEX(FAANUL_SIGN)
   ```

   Skrócona postać podpisu w postaci szesnastkowej:

   ```
   FAANUL_SIGN_HEX => 9e61a538a24334c0 … 03e51453caa1c8f3
   ```

   Pełną postać podpisu w postaci szesnastkowej należy zapisać w strukturze JSON w polu "RSA":

   ```
   faAnul/podpis/RSA => FAANUL_SIGN_HEX
   ```

A.10.2 Wyznaczanie wartości funkcji skrótu dokumentów przesyłanych w zbiorach danych:

Poniżej przedstawiono sposób wyliczania wartości skrótu SHA2 funkcją SHA-256 bieżącego dokumentu na podstawie skrótu poprzedniego dokumentu oraz podpisu bieżącego dokumentu. Wyliczane skróty służą do weryfikowania ciągłości łańcucha dokumentów tego samego typu przesyłanych w zbiorach danych, czyli paragonów fiskalnych anulowanych oraz raportów fiskalnych dobowych. Poniżej przedstawiono przykłady oparte na paragonach anulowanych, a identyczna zasada dotyczy raportów fiskalnych dobowych.

A.10.2a Wyliczenie wartości skrótu pierwszego paragonu anulowanego:

1. Przygotowanie danych do wyliczenia skrótu w przypadku pierwszego dokumentu polega na pobraniu podpisu bieżącego dokumentu:

   ```
   PARAGANUL_SHA_INPUT => PARAGANUL_SIGN
   ```

   Skrócona postać podpisu bieżącego dokumentu w postaci szesnastkowej:

```
PARAGANUL_SIGN_HEX => 9e61a538a24334c0 … 03e51453caa1c8f3
```

Pełna postać podpisu bieżącego dokumentu w postaci szesnastkowej przedstawiona jest w punkcie C.2.4d.

Skrócona postać danych wejściowych w postaci szesnastkowej:

```
PARAGANUL_SHA_INPUT => 9e61a538a24334c0 … 03e51453caa1c8f3
```

Pełna postać przykładowych danych wejściowych w postaci szesnastkowej przedstawiona jest w punkcie C.2.5a.

2. Wyliczenie wartości skrótu SHA2 funkcją skrótu SHA-256 dla przygotowanych danych:

```
PARAGANUL_SHA => SHA256(PARAGANUL_SHA_INPUT)
```

Otrzymany wynik zapisywany jest w postaci szesnastkowej:

```
PARAGANUL_SHA_HEX => HEX(PARAGANUL_SHA)
```

Wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona dla pełnych danych wejściowych:

```
eee0e3068482a34527630f4c73c05d0d3523899f5fa25d022b9415ff8057d3be
```

Otrzymany skrótu w postaci szesnastkowej należy zapisać w strukturze JSON w polu "SHA":

```
paragAnul/podpis/SHA => PARAGANUL_SHA_HEX
```

Dodatkowo w strukturze JSON w polu "JPK" należy wpisać identyfikator poprzedniego dokumentu, a jeżeli jest to pierwszy dokument danego typu to wpisujemy osiemnaście zer:

```
paragAnul/podpis/JPK => 000000000000000000
```

A.10.2b Wyliczenie wartości skrótu drugiego paragonu anulowanego:

1. Przygotowanie danych do wyliczenia skrótu polegające na bajtowym połączeniu skrótu poprzedniego dokumentu i podpisu bieżącego:

```
PARAGANUL_SHA_INPUT => PARAGANUL_SHA_PREV||PARAGANUL_SIGN
```

Opierając się na przykładowych danych z punktu C.2.1a skrót poprzedniego dokumentu, wyliczony w punkcie A.10.2a wynosi:

```
PARAGANUL_SHA_PREV => eee0e3068482a34527630f4c73c05d0d3523899f5fa25d022b9415ff8057d3be
```

Skrócona postać podpisu bieżącego dokumentu w postaci szesnastkowej:

```
PARAGANUL_SIGN_HEX => ab6c66f6f3cbc34d … cdb694b9afb0ebf3
```

Pełna postać podpisu bieżącego dokumentu w postaci szesnastkowej przedstawiona jest w punkcie C.2.4e.

Skrócona postać danych wejściowych w postaci szesnastkowej:

```
PARAGANUL_SHA_INPUT => eee0e3068482a345 … cdb694b9afb0ebf3
```

Pełna postać przykładowych danych wejściowych w postaci szesnastkowej przedstawiona jest w punkcie C.2.5b.

2. Wyliczenie wartości skrótu SHA2 funkcją skrótu SHA-256 dla przygotowanych danych:

```
PARAGANUL_SHA => SHA256(PARAGANUL_SHA_INPUT)
```

Otrzymany wynik zapisywany jest w postaci szesnastkowej:

```
PARAGANUL_SHA_HEX => HEX(PARAGANUL_SHA)
```

Wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona dla pełnych danych wejściowych:

```
a64a913986f2a18d4db5ecbe02309fc96d19c683830622140a2d4310425f911c
```

Otrzymany skrótu w postaci szesnastkowej należy zapisać w strukturze JSON w polu "SHA":

```
paragAnul/podpis/SHA => PARAGANUL_SHA_HEX
```

Dodatkowo w strukturze JSON w polu "JPK" należy wpisać identyfikator poprzedniego dokumentu. Opierając się na przykładowych danych z punktu C.2.1a, identyfikator pamięci chronionej poprzedniego dokumentu pamiecChr = 1, a identyfikator pierwszego paragonu anulowanego JPKID = 6, dlatego identyfikator poprzedniego dokumentu wynosi:

```
paragAnul/podpis/JPK => 0010000000000000006
```

A.10.2c Wyliczenie wartości skrótu trzeciego paragonu anulowanego:

1. Przygotowanie danych do wyliczenia skrótu polegające na bajtowym połączeniu skrótu poprzedniego dokumentu i podpisu bieżącego:

```
PARAGANUL_SHA_INPUT => PARAGANUL_SHA_PREV||PARAGANUL_SIGN
```

Opierając się na przykładowych danych z punktu C.2.1a skrót poprzedniego dokumentu, wyliczony w punkcie A.10.2b wynosi:

```
PARAGANUL_SHA_PREV => a64a913986f2a18d4db5ecbe02309fc96d19c683830622140a2d4310425f911c
```

Skrócona postać podpisu bieżącego dokumentu w postaci szesnastkowej:

```
PARAGANUL_SIGN_HEX => 54ce7bad1079bc8a … 73a937ec2f1ca93f
```

Pełna postać podpisu bieżącego dokumentu w postaci szesnastkowej przedstawiona jest w punkcie C.2.4f.

Skrócona postać danych wejściowych w postaci szesnastkowej:

```
PARAGANUL_SHA_INPUT => a64a913986f2a18d … 73a937ec2f1ca93f
```

Pełna postać przykładowych danych wejściowych w postaci szesnastkowej przedstawiona jest w punkcie C.2.5c.

2. Wyliczenie wartości skrótu SHA2 funkcją skrótu SHA-256 dla przygotowanych danych:

```
PARAGANUL_SHA => SHA256(PARAGANUL_SHA_INPUT)
```

Otrzymany wynik zapisywany jest w postaci szesnastkowej:

```
PARAGANUL_SHA_HEX => HEX(PARAGANUL_SHA)
```

Wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona dla pełnych danych wejściowych:

```
ac6450833bef0f47888dea1272d179e8a197c8b6968c16782eeaff4f2769430d
```

Otrzymany skrótu w postaci szesnastkowej należy zapisać w strukturze JSON w polu "SHA":

```
paragAnul/podpis/SHA => PARAGANUL_SHA_HEX
```

Dodatkowo w strukturze JSON w polu "JPK" należy wpisać identyfikator poprzedniego dokumentu. Opierając się na przykładowych danych z punktu C.2.1a, identyfikator pamięci chronionej poprzedniego dokumentu pamiecChr = 1, a identyfikator drugiego paragonu anulowanego JPKID = 9, dlatego identyfikator poprzedniego dokumentu wynosi:

```
paragAnul/podpis/JPK => 0010000000000000009
```

A.10.3 Podpisywanie dokumentów w postaci elektronicznej:

Poniżej przedstawiono sposób podpisywania dokumentów w postaci elektronicznej wysyłanych z kasy rejestrującej online lub kasy rejestrującej w postaci oprogramowania do repozytorium oraz na życzenie do klienta, równoważny opisowi podpisywania danych przesyłanych do repozytorium A.4, a wzorowany na opisie zawartym w załączniku A.2 specyfikacji RFC 7515.

1. Przygotowanie chronionego nagłówka podpisu (JWS Protected Header):
   - wyszczególnienie użytego algorytmu podpisu w parametrze ”*alg*”,
   - dodanie parametru ”*x5c*” zawierającego zgodnie z opisem w sekcji 4.1.6 dokumentu RFC 7515 jednoelementową tablicę JSON z certyfikatem klucza publicznego użytym do podpisu, w formacie DER zakodowanym Base64 bez znacznika początku i końca certyfikatu oraz bez znaków końca linii,

   UWAGA: ciąg znaków reprezentujący certyfikat może zostać poszerzony o wstawienie znaku specjalnego ‘\’ poprzedzającego znak ‘/’,
   - dodanie parametru *”eParagon.mf.gov.pl”* zawierającego zakodowany w Base64 obiekt JSON składający się z parametrów:
     - JPKID - identyfikatora bieżącego dokumentu (wraz z numerem pamięci chronionej),
     - wersja - wersji schematu użytej struktury JSON,
     - dataJPK - daty i czasu wystawienia dokumentu,
     - JPKREF - elementu zawierającego:
       - JPKID - identyfikator poprzedniego dokumentu (wraz z numerem pamięci chronionej),
       - SHA256 - wartość funkcji skrótu poprzedniego dokumentu,
   - dodanie opcjonalnego parametru ”*jpkmetadata*” zawierającego zakodowany w Base64 obiekt JSON składający się z opcjonalnych parametrów:

- correlationId - numer korelacyjny, czyli identyfikator ”*commandId*” wykonywanej komendy pobranej z usługi WebApi,
- compression - metoda kompresowania przesyłanych danych:
  - DEFLATE - kompresja algorytmem opisanym w dokumencie RFC 1951,
  - NONE – przesłanie nieskompresowanych danych,
  - brak parametru ”compression” oznacza brak kompresji danych.

UWAGA: ciąg znaków reprezentujący metadane może zostać poszerzony o wstawienie znaku specjalnego ‘\’ poprzedzającego znak ‘/’.

Skrócona postać nagłówka w formacie JSON:

```
JWS_PH => {"alg": "RS256", "x5c": ["MIID … Rw=="], "eParagon.mf.gov.pl": "eyJ3 … In19",
                                                                  "jpkmetadata": "eyJj … In0="}
```

Pełna postać z wykorzystaniem certyfikatu testowego przedstawiona jest w punkcie C.3.1.

Zgodnie z punktem 4.1 parametr ”alg” przyjmuje wartość ”RS256”, ponieważ do podpisania dokumentu należy użyć algorytmu asymetrycznego RSA z dopełnieniem PKCS1 w wersji 1.5.

W parametrze ”x5c” zamieszczono certyfikat klucza publicznego (punkt C.1.2) testowej kasy w postaci oprogramowania w formie jednoelementowej tablicy w formacie DER zakodowanym Base64 bez znacznika początku i końca certyfikatu oraz bez znaków końca.

W parametrach ”*eParagon.mf.gov.pl*” oraz ”jpkmetadata” zamieszczono zakodowane w Base64 odpowiednie struktury JSON.

Przykładowa postać parametru ”*eParagon.mf.gov.pl*” w formacie JSON:

```
a) paragon pierwszy
{
    "wersja": "JPK_KASA_PARAGON_v1-0",
    "JPKID": "001000000000000004",
    "dataJPK": "2020-04-10T04:23:45.678Z",
    "JPKREF": {
        "SHA256": "0000000000000000000000000000000000000000000000000000000000000000",
        "JPKID": "000000000000000000"
    }
}

b) paragon drugi
{
    "wersja": "JPK_KASA_PARAGON_v1-0",
    "JPKID": "001000000000000005",
    "dataJPK": "2020-04-10T05:23:45.678Z",
    "JPKREF": {
        "SHA256": "F88E6E5AD956195072FC437954AB3BA05F0F3FF677F6A0129CB9EFFC83538BA0",
        "JPKID": "001000000000000004"
    }
}

c) paragon trzeci
{
    "wersja": "JPK_KASA_PARAGON_v1-0",
    "JPKID": "001000000000000007",
    "dataJPK": "2020-04-10T07:23:45.678Z",
    "JPKREF": {
        "SHA256": "7769C389BB33C7F34B06D1CB6C0DA13F9AD30585BFE47B7DB085A2A26890E101",
        "JPKID": "001000000000000005"
    }
```

```
}

d) paragon czwarty
{
    "wersja": "JPK_KASA_PARAGON_v1-0",
    "JPKID": "0010000000000000008",
    "dataJPK": "2020-04-10T08:23:45.678Z",
    "JPKREF": {
        "SHA256": "BBF43DA8F1BB31AE6F3149905732C50AD7A88BC6A2CE2A9360B45CBC1CDCF0F1",
        "JPKID": "0010000000000000007"
    }
}
```

Przykładowa postać parametru *"jpkmetadata"* w formacie JSON:

```
{"correlationId":"TFD.WTE2001000009.2020-04-03T11:50:00.322Z"}

{"correlationId":"TFD.WTE2001000009.2020-04-03T11:50:00.322Z","compression":"NONE"}

{"correlationId":"TFD.WTE2001000009.2020-04-03T11:50:00.322Z","compression":"DEFLATE"}
```

2. Przygotowany nagłówek przekształcany jest przez kodowanie Base64URL:

```
JWS_PH_URL => BASE64URL(JWS_PH)
```

Pełna postać nagłówka zakodowanego Base64URL przedstawiona jest w punkcie C.3.2.

3. Przygotowanie zawartości danych do podpisu i opcjonalnie skompresowanie:

```
JWS_DATA => { "dokument": { "naglowek": {…}, "podmiot1": {…}, "paragon": { … } } }

opcjonalnie skompresowanie:

JWS_DATA => DEFLATE(JWS_DATA)
```

Pełna postać przykładowych ustrukturyzowanych danych przedstawiona jest w punkcie C.3.3.

Pełna postać przykładowych nieskompresowanych danych przedstawiona jest w punkcie C.3.4.

4. Przygotowane dane należy zakodować w Base64URL:

```
JWS_DATA_URL => BASE64URL(JWS_DATA)
```

Pełna postać przykładowych danych zakodowanych Base64URL przedstawiona jest w punkcie C.3.5.

5. Przygotowanie zawartości do popisu polegające na połączeniu nagłówka i danych zakodowanych w Base64URL rozdzielonych kropką:

```
JWS_SIGNING_INPUT => JWS_PH_URL||.||JWS_DATA_URL
```

6. Tworzenie podpisu z wykorzystaniem algorytmu RSA oraz klucza prywatnego kasy i zakodowanie podpisu Base64URL:

```
JWS_SIGN_URL => BASE64URL(RS256(JWS_SIGNING_INPUT,RSA_PRIVATE_KEY))
```

7. Przygotowanie obiektu JWS polegające na połączeniu danych do podpisu i otrzymanego podpisu zakodowanych w Base64URL rozdzielonych kropką:

```
JWS => JWS_SIGNING_INPUT||.||JWS_SIGN_URL
```

albo

```
JWS => JWS_PH_URL||.||JWS_DATA_URL||.||JWS_SIGN_URL
```

Pełna postać przykładowego obiektu JWS z wykorzystaniem certyfikatu C.1.2 przedstawiona jest w punkcie C.3.6.

A.10.4 Wyznaczanie wartości funkcji skrótu dokumentów w postaci elektronicznej:

Poniżej przedstawiono sposób wyliczania wartości skrótu SHA2 funkcją SHA-256 bieżącego dokumentu na podstawie skrótu poprzedniego dokumentu oraz podpisu bieżącego dokumentu. Wyliczane skróty służą do weryfikowania ciągłości łańcucha dokumentów tego samego typu.

Przygotowanie danych do wyliczenia skrótu polega na pobraniu całego obiektu JWS ponieważ zawiera on podpis bieżącego dokumentu jak również skrót poprzedniego:

```
PARAGON_SHA_INPUT => PARAGON_JWS
```

Skrócona postać dokumentu w postaci elektronicznej:

```
PARAGON_SHA_INPUT => eyJlUGFyYWdvbi5t … aXwz4zui_fOrXxsg
```

Pełna postać dokumentu w postaci elektronicznej przedstawiona jest w punkcie C.3.6.

Wyliczenie wartości skrótu SHA2 funkcją skrótu SHA-256 dla przygotowanych danych:

```
PARAGON_SHA => SHA256(PARAGON_SHA_INPUT)
```

Otrzymany wynik zapisany w postaci szesnastkowej:

```
PARAGON_SHA_HEX => HEX(PARAGON_SHA)
```

a) wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona dla dokumentu elektronicznego z punktu C.3.6a:

```
f88e6e5ad956195072fc437954ab3ba05f0f3ff677f6a0129cb9effc83538ba0
```

b) wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona dla dokumentu elektronicznego z punktu C.3.6b:

```
7769c389bb33c7f34b06d1cb6c0da13f9ad30585bfe47b7db085a2a26890e101
```

c) wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona dla dokumentu elektronicznego z punktu C.3.6c:

```
bbf43da8f1bb31ae6f3149905732c50ad7a88bc6a2ce2a9360b45cbc1cdcf0f1
```

d) wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona dla dokumentu elektronicznego z punktu C.3.6d:

```
ebc3974cde25a119e123f6661e5c8d51670c735d4c10b123b2d4e57befe4021c
```

Otrzymany skrótu w postaci szesnastkowej należy zapisać w nagłówku następnego dokumentu danego typu w postaci elektronicznej. Zapisu należy dokonać w nagłówku obiektu JWS w parametrze ”*eParagon.mf.gov.pl*” w polu "SHA256":

```
JPKREF/SHA256 => PARAGON_SHA_HEX
```

W punkcie A.10.3 przedstawiono przykładowe postaci parametru *”eParagon.mf.gov.pl”*, w których odpowiednio zawarto obliczone powyżej skróty SHA2. Mianowicie skrót pierwszego paragonu zawarto w nagłówku drugiego paragonu, skrót drugiego paragonu zawarto w nagłówku trzeciego paragonu i skrót trzeciego paragonu zawarto w nagłówku czwartego paragonu. Nagłówek pierwszego paragonu zawiera parametr *”eParagon.mf.gov.pl”*, którego pola "JPKREF/SHA256" i "JPKREF/JPKID" zawierają same zera odpowiednio sześćdziesiąt cztery oraz osiemnaście wskazujące, że jest to pierwszy dokument danego typu i nie posiada poprzednika.

A.10.5 Weryfikacja ciągłości łańcucha dokumentów w kasach w postaci oprogramowania:

Poniżej przedstawiono sposób weryfikacji ciągłości łańcucha zarówno dokumentów w postaci elektronicznej, czyli paragonów fiskalnych jak i dokumentów przesyłanych w zbiorach danych (paragonów fiskalnych anulowanych i raportów fiskalnych dobowych).

Mechanizm weryfikacji ciągłości łańcucha paragonów fiskalnych opiera się na porównaniu obliczonej wartości skrótu SHA2 funkcją SHA-256 poprzednika z wartością zawartą w bieżącym dokumencie. Natomiast weryfikacja ciągłości łańcucha paragonów fiskalnych anulowanych i raportów fiskalny dobowych polega na wyliczeniu wartości skrótu SHA2 funkcją SHA-256 poprzednika, a następnie wyliczeniu wartości skrótu SHA2 funkcją SHA-256 bieżącego dokumentu na podstawie skrótu poprzedniego dokumentu oraz podpisu bieżącego dokumentu i porównaniu otrzymanego wyniku ze skrótem SHA2 bieżącego dokumentu zapisanym w strukturze JSON.

1. Weryfikacja łańcucha dokumentów w postaci elektronicznej - paragonów fiskalnych:

   W załączniku C w punkcie C.3.6 zamieszczono przykład sekwencji czterech paragonów fiskalnych z możliwością weryfikacji łańcucha dokumentów. Rozpoczynając od ostatniego (czwartego) paragonu należy obliczyć skrót poprzednika o ile istnieje i porównać z wartością zapisaną w nagłówku bieżącego dokumentu.

   W paragonie czwartym w nagłówku JWS parametr *”eParagon.mf.gov.pl”* ma postać:

```
{
    "wersja": "JPK_KASA_PARAGON_v1-0",
    "JPKID": "0010000000000000008",
    "dataJPK": "2020-04-10T08:23:45.678Z",
    "JPKREF": {
        "SHA256": "BBF43DA8F1BB31AE6F3149905732C50AD7A88BC6A2CE2A9360B45CBC1CDCF0F1",
        "JPKID": "0010000000000000007"
    }
}
```

   Z powyższego należy wywnioskować iż poprzednik będzie charakteryzował się wartościami:

```
PARAGON_REF_SHA_HEX => BBF43DA8F1BB31AE6F3149905732C50AD7A88BC6A2CE2A9360B45CBC1CDCF0F1
PARAGON_REF_PAMIEC_CHR => 001 => 1
PARAGON_REF_JPKID => 000000000000007 => 7
```

   Opierając się na przykładowych danych z punktu C.3.3, można zidentyfikować iż poprzednim paragonem był paragon trzeci zawierający identyfikator dokumentu JPKID równy 7, punkt C.3.3c:

```
/dokument/paragon/pamiecChr == 1
/dokument/paragon/JPKID == 7
```

   W związku z tym dla jego postaci elektronicznej (całego obiektu JWS) należy wyliczyć skrót SHA2:

```
PREV_PARAGON_SHA => SHA256(PREV_PARAGON_JWS)
```

Otrzymany wynik w postaci szesnastkowej:

```
PREV_PARAGON_SHA_HEX => HEX(PREV_PARAGON_SHA)
```

Wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona dla dokumentu z punktu C.3.6c:

```
bbf43da8f1bb31ae6f3149905732c50ad7a88bc6a2ce2a9360b45cbc1cdcf0f1
```

```
PARAGON_REF_SHA_HEX  - BBF43DA8F1BB31AE6F3149905732C50AD7A88BC6A2CE2A9360B45CBC1CDCF0F1
PREV_PARAGON_SHA_HEX - bbf43da8f1bb31ae6f3149905732c50ad7a88bc6a2ce2a9360b45cbc1cdcf0f1
```

Porównując wyliczoną wartość ze skrótem zawartym w nagłówku dokonuje się weryfikacji sekwencji i w przypadku poprawnej powtarza się opisany algorytm traktując poprzednika jako bieżący dokument. Iterację można przeprowadzać dla wybranej liczby dokumentów lub do osiągnięcia pierwszego dokumentu, który nie posiada poprzednika. Wystąpienie rozbieżności przy porównywaniu skrótów SHA2 świadczy jednoznacznie o niepoprawnym utworzeniu łańcucha dokumentów.

2. Weryfikacja łańcucha dokumentów przesyłanych w zbiorach danych:

   W załączniku C w punktach C.2.2d, C.2.2e oraz C.2.2f zamieszczono przykład sekwencji trzech paragonów fiskalnych anulowanych z możliwością weryfikacji łańcucha dokumentów. Rozpoczynając od ostatniego (C.2.2f) paragonu anulowanego należy uzyskać skrót poprzednika o ile istnieje i połączyć bajtowo z podpisem bieżącego paragonu anulowanego, a z otrzymanej tablicy bajtów wyliczyć skrót SHA-256 i porównać z wartością zapisaną w bieżącym dokumencie.

   W strukturze JSON paragonu anulowanego element ”*podpis*” zawiera odpowiednie dane:

   Fragment struktury JSON poprzedniego paragonu anulowanego C.2.2f:

```
"paragAnul": {
    "JPKID": 10,
    "pamiecChr": 1,
…
    "podpis": {
        "RSA": "54ce7bad … 2f1ca93f",
        "SHA": "ac6450833bef0f47888dea1272d179e8a197c8b6968c16782eeaff4f2769430d",
        "JPK": "0010000000000000009"
    }
}
```

   Z powyższego należy pobrać weryfikowany skrót SHA oraz podpis potrzebny do weryfikacji:

```
PARAGANUL_SHA_HEX => ac6450833bef0f47888dea1272d179e8a197c8b6968c16782eeaff4f2769430d
PARAGANUL_RSA_HEX => 54ce7bad … 2f1ca93f
```

   Dodatkowo należy wywnioskować iż poprzednik będzie charakteryzował się wartościami:

```
PARAGANUL_REF_PAMIEC_CHR => 001 => 1
PARAGANUL_REF_JPKID => 000000000000009 => 9
```

Opierając się na powyższych danych można zidentyfikować iż poprzednim paragonem anulowanym był paragon zawierający identyfikator dokumentu JPKID równy 9, punkt C.2.2e:

```
//paragAnul/pamiecChr == 1
//paragAnul/JPKID == 9
```

Fragment struktury JSON poprzedniego paragonu anulowanego C.2.2e:

```
"paragAnul": {
    "JPKID": 9,
    "pamiecChr": 1,
…
    "podpis": {
        "RSA": "ab6c66f6 … afb0ebf3",
        "SHA": "a64a913986f2a18d4db5ecbe02309fc96d19c683830622140a2d4310425f911c",
        "JPK": "0010000000000000006"
    }
}
```

Ze wskazanego dokumentu należy pobrać skrót SHA:

```
PREV_PARAGANUL_SHA => a64a913986f2a18d4db5ecbe02309fc96d19c683830622140a2d4310425f911c
```

Następnie połączyć bajtowo z podpisem bieżącego dokumentu:

```
PARAGANUL_INPUT => PREV_PARAGANUL_SHA||PARAGANUL_RSA_HEX
```

W celu wyliczenia i weryfikacji skrótu SHA analizowanego dokumentu:

```
PARAGANUL_INPUT_SHA => SHA256(PARAGANUL_INPUT)
```

Otrzymany wynik w postaci szesnastkowej:

```
PARAGANUL_INPUT_SHA_HEX => HEX(PARAGANUL_INPUT_SHA)
```

Wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona dla dokumentu z punktu C.2.5c:

```
ac6450833bef0f47888dea1272d179e8a197c8b6968c16782eeaff4f2769430d

PARAGANUL_SHA_HEX       - ac6450833bef0f47888dea1272d179e8a197c8b6968c16782eeaff4f2769430d
PARAGANUL_INPUT_SHA_HEX - ac6450833bef0f47888dea1272d179e8a197c8b6968c16782eeaff4f2769430d
```

Porównując wyliczoną wartość ze skrótem zawartym w strukturze JSON bieżącego dokumentu w elemencie ”podpis” dokonuje się weryfikacji sekwencji i w przypadku poprawnej powtarza się opisany algorytm traktując poprzednika jako bieżący dokument. Iterację można przeprowadzać dla wybranej liczby dokumentów lub do osiągnięcia pierwszego dokumentu, który nie posiada poprzednika. Wystąpienie rozbieżności przy porównywaniu skrótów SHA2 świadczy jednoznacznie o niepoprawnym utworzeniu łańcucha dokumentów.

A.10.6 Tworzenie kodu weryfikującego dokument kasy w postaci oprogramowania:

Poniżej przedstawiono sposób tworzenia kodu weryfikującego paragon fiskalny na podstawie klucza współdzielonego oraz odpowiednich danych jednoznacznie identyfikujących dokument.

1. Przygotowanie danych identyfikujących paragon fiskalny, czyli wartość funkcji skrótu dokumentu, numer unikatowy kasy, numer kolejny dokumentu (JPKID wraz z numerem pamięci chronionej), znacznik czasu odzwierciedlający datę i czas zakończenia sprzedaży.

   Wyliczenie skrótu paragonu fiskalnego (całego obiektu JWS) opisane w punkcie A.10.4:

   ```
   PARAGON_SHA_INPUT => PARAGON_JWS
   ```

   Skrócona postać dokumentu w postaci elektronicznej:

   ```
   PARAGON_SHA_INPUT => eyJlUGFyYWdvbi5t … aXwz4zui_fOrXxsg
   ```

   Pełna postać dokumentu w postaci elektronicznej przedstawiona jest w punkcie C.3.6a.

   Wyliczenie wartości skrótu SHA2 funkcją skrótu SHA-256 dla przygotowanych danych:

   ```
   PARAGON_SHA => SHA256(PARAGON_SHA_INPUT)
   ```

   Otrzymany wynik zapisany w postaci szesnastkowej:

   ```
   PARAGON_SHA_HEX => HEX(PARAGON_SHA)
   ```

   Wartość funkcji skrótu SHA-256 w formacie szesnastkowym obliczona dla dokumentu elektronicznego z punktu C.3.6a:

   ```
   PARAGON_SHA_HEX => f88e6e5ad956195072fc437954ab3ba05f0f3ff677f6a0129cb9effc83538ba0
   ```

   Numer unikatowy kasy przydzielony jest każdej kasie i zapisany w bazie danych kasy oraz wysyłany w strukturach danych w formacie JSON. Opierając się na przykładowych danych z punktu C.3.3a kasy testowej numer unikatowy przyjmuje wartość:

   ```
   PARAGON_NR_UNIK => /dokument/podmiot1/nrUnik => WTE2001000009
   ```

   Zamieniając powyższą wartość w tablicę bajtową otrzymamy poniższą postać szesnastkową:

   ```
   PARAGON_NR_UNIK_HEX => 57544532303031303030303039
   ```

   Pozostałe dane zawarte są zarówno w dokumencie jak również w nagłówku JWS w parametrze ”*eParagon.mf.gov.pl*”, który dla paragony pierwszego z punktu C.3.6a ma postać:

   ```
   {
       "wersja": "JPK_KASA_PARAGON_v1-0",
       "JPKID": "0010000000000000004",
       "dataJPK": "2020-04-10T04:23:45.678Z",
       "JPKREF": {
           "SHA256": "0000000000000000000000000000000000000000000000000000000000000000",
           "JPKID": "000000000000000000"
       }
   }
   ```

   W związku z tym numer kolejny dokumentu (JPKID wraz z numerem pamięci chronionej) oraz znacznik czasu odzwierciedlający datę i czas zakończenia sprzedaży przyjmą wartości:

   ```
   PARAGON_JPKID => 001000000000000004
   PARAGON_DATA_JPK => 2020-04-10T04:23:45.678Z
   ```

Powyższe wartości w postaci liczby całkowitej (data jako UNIX timestamp w milisekundach):

```
PARAGON_JPKID => 1000000000000004
PARAGON_DATA_JPK => 1586492625678
```

Obie wartości należy przedstawić w postaci ośmiobajtowej tablicy - postać szesnastkowa:

```
PARAGON_JPKID_HEX => 00038d7ea4c68004
PARAGON_DATA_JPK_HEX => 000001716254530e
```

Przykładowy klucz współdzielony w środowisku testowym wygenerowany dla kasy testowej:

```
PARAGON_SHARED_KEY_B64 => gZ5ff8DkMdgdLJGqC54Qh3PONDbOF2Fp6D0VVLwd3oY=
PARAGON_SHARED_KEY_HEX => 819e5f7fc0e431d81d2c91aa0b9e108773ce3436ce176169e83d1554bc1dde86
```

2. Wyliczenia kodu autoryzacyjnego należy dokonać bazując na połączeniu bajtowym powyższych danych i kluczu współdzielonym w funkcji haszującej HS256:

```
PARAGON_SHA_HEX => f88e6e5ad956195072fc437954ab3ba05f0f3ff677f6a0129cb9effc83538ba0
PARAGON_NR_UNIK_HEX => 57544532303031303030303039
PARAGON_JPKID_HEX => 00038d7ea4c68004
PARAGON_DATA_JPK_HEX => 000001716254530e

PARAGON_VERIFY_DATA_HEX =>
PARAGON_SHA_HEX||PARAGON_NR_UNIK_HEX||PARAGON_JPKID_HEX||PARAGON_DATA_JPK_HEX

PARAGON_VERIFY_DATA_HEX =>
f88e6e5ad956195072fc437954ab3ba05f0f3ff677f6a0129cb9effc83538ba057544532303031303030303039
00038d7ea4c680040000001716254530e
```

Wynik użycia powyższego ciągu bajtów oraz klucza współdzielonego w funkcji haszującej HS256 w wyniku zwróci kod autoryzacyjny o wartości w postaci szesnastkowej:

```
PARAGON_VERIFY_CODE_HEX =>
db7d31eda33af45020f8a388b09737a5a836c6dee1be16e23d9e2c7441539a93
```

3. Utworzenie kodu weryfikującego polega na połączeniu bajtowo danych weryfikujących i kodu autoryzacyjnego:

```
PARAGON_QR_CODE_HEX =>
f88e6e5ad956195072fc437954ab3ba05f0f3ff677f6a0129cb9effc83538ba057544532303031303030303039
00038d7ea4c680040000001716254530edb7d31eda33af45020f8a388b09737a5a836c6dee1be16e23d9e2c7441
539a93
```

po przekodowaniu do formatu Base64URL:

```
PARAGON_QR_CODE_URL =>
-
I5uWtlWGVBy_EN5VKs7oF8PP_Z39qASnLnv_INTi6BXVEUyMDAxMDAwMDA5AAONfqTGgAQAAAFxYlRTDtt9Me2jOvR
QIPijiLCXN6WoNsbe4b4W4j2eLHRBU5qT
```

Poniżej przykład wizualizacji kodu weryfikującego w postaci QR Code w wersji 6:

Załącznik B

B.1 Przykładowe certyfikaty środowiska testowego

B.1.1 Certyfikat klucza publicznego ministerstwa do podpisywania komend oraz szyfrowania klucza szyfrującego przesyłanych danych z kasy fiskalnej do repozytorium:

```
-----BEGIN CERTIFICATE-----
MIIFHDCCAwSgAwIBAgITOgAAAAjmj1WBXU6mOgABAAAACDANBgkqhkiG9w0BAQ0F
ADAWMRQwEgYDVQQDEwtlS2FzeS1TdWJDQTAgFw0xNzA4MjIwNjMzMTNaGA8yMDky
MDcxMDEyMjcyOVowgcgxCzAJBgNVBAYTAlBMMRQwEgYDVQQIEwtNYXpvd2llY2tp
ZTERMA8GA1UEBxMIV2Fyc3phd2ExHzAdBgNVBAoMFk1pbmlzdGVyc3R3byBGaW5h
bnPDs3cxIzAhBgNVBAsTGkRlcGFydGFtZW50IEluZm9ybWF0eXphY2ppMR4wHAYD
VQQDExV0ZXN0LWUta2FzeS5tZi5nb3YucGwxKjAoBgkqhkiG9w0BCQEWG2luZm8u
ZS1kZWtsYXJhY2plQG1mLmdvdi5wbDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMvyVXGj8YNhy6P28bKj9MleA7+QXKCtPJZ4M6MIxiaqA4lodd9No+Ws
gRETVzEPiB8raL9n3uM+RBFwK2A4VvuAWuGZx2drkfMZnpSVFLOsQnadB1rjBCY5
G/pMX6eI7Bltx4XFYK/1cY1U+mFVc94Ryfyxyy0ZWSD8IGV9n0AilDpRfIJBOu5a
3oquz8ZZGuWyU95KWBKRAD7SV2bpTlYWX4UHhTe323HTYL3rDbKP73HAoylObSmS
vmB9MyNzWgBf73UOHmzXPqpuRbLFnR+llTA0FA8kOylxtijygMXpICOai7av2ofG
t65v0GJg5wlJuqWvkQXFUyoyGGUYaQsCAwEAAaOBrTCBqjAdBgNVHQ4EFgQUx7xK
j1TXCorOExa2hY/jdz6NkA0wHwYDVR0jBBgwFoAUBb+Partd6TV4PV1kTUrtJads
SdowWgYIKwYBBQUHAQEETjBMMEoGCCsGAQUFBzAChj5maWxlOi8vLy9zYXAtd2lu
LTgyNi9DZXJ0RW5yb2xsL3NhcC13aW4tODI2X2VLYXN5LVN1YkNBKDEpLmNydDAM
BgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBDQUAA4ICAQCkdUR2DhgiexUW+y2rgaE6
orWBPyMxveH2IPv0rPGzqdgUFcNH816YzDorEnOAvbRLB8BaoH+Wn/eElAQxqE5+
47VgScIUF4oNHwXnnflR1XRoYcFZ/fBkIW2nfOK1C8y2vHtZG1QEyyVD/cxv7ubg
OiJfOYScsHv5DItStFUBclvg3xrFi2zG5ahblMwqCGrvgPKOxR9+mXGD+eoThBHE
P6aJF3Zu41mVwT/4cbSr5m3c77deEQ2CpQPGL874PiHy9omkjev9F5yoBzI7ypha
lyEIdbASU0UiUErjbS+hnw0RErV1bQQzQfS7qiKMBZTM4pzOv/Ro6f+OcBf7c16X
tHrEgli/aNagKo34nFhUscQcUTCh3MsCKuVSZU3dbCdSLIvdoJIS5FLP+gr8LbQW
9uR/NgwJhYr/w06k6AOF+TaJw8eakv5ELDOuzhipqB63BuMSCGFZcUQ2bDhdc5gc
V9GlNgVEXmToee3fn89OQTC7GrCwFzNxwAM6gJ0MARyWl5Hmgr/pOb1MX5Vehgao
HpjoveMAacONbtiOwfMUyhPdCJmnLP67lokvGq7PDJ/DUbespAqVm91TM6QbWjda
nKGB6kJY+7H5ESI8sp/nzjHXdZxeIPO7lOTItKdRW82kRcBR9TNDSS6rt5sI16LW
0NCJ2zprYt8XrNO728ljyA==
-----END CERTIFICATE-----
```

B.1.2 Certyfikat klucza publicznego kasy fiskalnej do podpisywania danych wytworzonych przez kasę oraz szyfrowania klucza szyfrującego przesyłanych komend wysyłanych do kasy:

```
-----BEGIN CERTIFICATE-----
MIICfjCCAeegAwIBAgIQzILUrkD2iqNCxC1ZrG7UBDANBgkqhkiG9w0BAQsFADAU
MRIwEAYDVQQDEwlNRiBlLUthc3kwHhcNMTcxMTE1MDk0MDAzWhcNMTkxMTE1MDk0
MDAyWjAYMRYwFAYDVQQDEw1aVEUxNzAxMDAwOTAxMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAwy3Kc3oTipU45lOIX6K3rruFY83vMqYJqwoWzrRVmZn8
5cNHSwoa/f96AW0/akADbJ3uo7U8oWhTF/rj8xIds4uimrN1YiPFmbXAMaeRQDbB
a/qvI5SRQtK9Bmse7KyspIFXVfEWP17OkDiBEZ/n+NC6ERzzKkxA3gMRQFGpHUSQ
2+EOi7kykPGi1f8Yh/2czd+FBvyrp8oSjyX951DdCsqG+rIwlz9p8PeoFwUggwhb
2tMl48U3nD9gZGXLuGOMBZ3nJ9U3fHVdi7XCpvn0PqvTSZLNL45yqXETu6bAZWB5
Ab4q5EVvI4unrjnJqc3fPD2OLXpINIssg6uqyTVCZQIDAQABo0kwRzBFBgNVHQEE
PjA8gBDGD6f6PWMBTV/bee5Lrlc9oRYwFDESMBAGA1UEAxMJTUYgZS1LYXN5ghCz
wtV5n24/mUCWe9d7xth6MA0GCSqGSIb3DQEBCwUAA4GBAKRTZFPJY5ObY4VVGpJL
l4Xb2JNtWpNXdwPs3N8I2rliGc0dxyq8R4C9X125G0GLgXXXTMDtnE1k+xmCk0aU
6bj2xpfezLhW6i1+mmHTB/2+JhsKp5oRRTXg8SpH5G1vwQI9ek9B/bYvn72nKrUa
Tp3PZsmCNqm1D0VayfTRhZiS
-----END CERTIFICATE-----
```

B.2 Przykładowe dane procesu podpisywania komendy w środowisku testowym

B.2.1 Pełna postać chronionego nagłówka podpisu komend przesyłanych do kasy:


```
{"alg":"RS256","x5c":["MIIFHDCCAwSgAwIBAgITOgAAAAjmj1WBXU6mOgABAAAACDANBgkqhkiG9w0BAQ0FADAWMRQ
wEgYDVQQDEwtlS2FzeS1TdWJDQTAgFw0xNzA4MjIwNjMzMTNaGA8yMDkyMDcxMDEyMjcyOVowgcgxCzAJBgNVBAYTAlBMM
RQwEgYDVQQIEwtNYXpvd2llY2tpZTERMA8GA1UEBxMIV2Fyc3phd2ExHzAdBgNVBAoMFk1pbmlzdGVyc3R3byBGaW5hbnP
Ds3cxIzAhBgNVBAsTGkRlcGFydGFtZW50IEluZm9ybWF0eXphY2ppMR4wHAYDVQQDExV0ZXN0LWUta2FzeS5tZi5nb3Yuc
GwxKjAoBgkqhkiG9w0BCQEWG2luZm8uZS1kZWtsYXJhY2plQG1mLmdvdi5wbDCCASIwDQYJKoZIhvcNAQEBBQADggEPADC
CAQoCggEBAMvyVXGj8YNhy6P28bKj9MleA7+QXKCtPJZ4M6MIxiaqA4lodd9No+WsgRETVzEPiB8raL9n3uM+RBFwK2A4V
vuAWuGZx2drkfMZnpSVFLOsQnadB1rjBCY5G/pMX6eI7Bltx4XFYK/1cY1U+mFVc94Ryfyxyy0ZWSD8IGV9n0AilDpRfIJ
BOu5a3oquz8ZZGuWyU95KWBKRAD7SV2bpTlYWX4UHhTe323HTYL3rDbKP73HAoylObSmSvmB9MyNzWgBf73UOHmzXPqpuR
bLFnR+llTA0FA8kOylxtijygMXpICOai7av2ofGt65v0GJg5wlJuqWvkQXFUyoyGGUYaQsCAwEAAaOBrTCBqjAdBgNVHQ4
EFgQUx7xKj1TXCorOExa2hY/jdz6NkA0wHwYDVR0jBBgwFoAUBb+Partd6TV4PV1kTUrtJadsSdowWgYIKwYBBQUHAQEET
jBMMEoGCCsGAQUFBzAChj5maWxlOi8vLy9zYXAtd2luLTgyNi9DZXJ0RW5yb2xsL3NhcC13aW4tODI2X2VLYXN5LVN1YkN
BKDEpLmNydDAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBDQUAA4ICAQCkdUR2DhgiexUW+y2rgaE6orWBPyMxveH2IPv0r
PGzqdgUFcNH816YzDorEnOAvbRLB8BaoH+Wn/eElAQxqE5+47VgScIUF4oNHwXnnflR1XRoYcFZ/fBkIW2nfOK1C8y2vHt
ZG1QEyyVD/cxv7ubgOiJfOYScsHv5DItStFUBclvg3xrFi2zG5ahblMwqCGrvgPKOxR9+mXGD+eoThBHEP6aJF3Zu41mVw
T/4cbSr5m3c77deEQ2CpQPGL874PiHy9omkjev9F5yoBzI7yphalyEIdbASU0UiUErjbS+hnw0RErV1bQQzQfS7qiKMBZT
M4pzOv/Ro6f+OcBf7c16XtHrEgli/aNagKo34nFhUscQcUTCh3MsCKuVSZU3dbCdSLIvdoJIS5FLP+gr8LbQW9uR/NgwJh
Yr/w06k6AOF+TaJw8eakv5ELDOuzhipqB63BuMSCGFZcUQ2bDhdc5gcV9GlNgVEXmToee3fn89OQTC7GrCwFzNxwAM6gJ0
MARyWl5Hmgr/pOb1MX5VehgaoHpjoveMAacONbtiOwfMUyhPdCJmnLP67lokvGq7PDJ/DUbespAqVm91TM6QbWjdanKGB6
kJY+7H5ESI8sp/nzjHXdZxeIPO7lOTItKdRW82kRcBR9TNDSS6rt5sI16LW0NCJ2zprYt8XrNO728ljyA=="]}
```


B.2.2 Pełna postać chronionego nagłówka podpisu komend przesyłanych do kasy fiskalnej zakodowana w Base64URL:


```
eyJhbGciOiJSUzI1NiIsIng1YyI6WyJNSUlGSERDQ0F3U2dBd0lCQWdJVE9nQUFBQWptajFXQlhVNm1PZ0FCQUFBQUNEQU
5CZ2txaGtpRzl3MEJBUTBGQURBV01SUXdFZ1lEVlFRREV3dGxTMkZ6ZVMxVGRXSkRRVEFnRncweE56QTRNakl3TmpNek1U
TmFHQTh5TURreU1EY3hNREV5TWpjeU9Wb3dnY2d4Q3pBSkJnTlZCQVlUQWxCTU1SUXdFZ1lEVlFRSUV3dE5ZWHB2ZDJsbF
kydHBaVEVSTUE4R0ExVUVCeE1JVjJGeWMzcGhkMkV4SHpBZEJnTlZCQW9NRmsxcGJtbHpkR1Z5YzNSM2J5QkdhVzVoYm5Q
RHMzY3hJekFoQmdOVkJBc1RHa1JsY0dGeWRHRnRaVzUwSUVsdVptOXliV0YwZVhwaFkycHBNUjR3SEFZRFZRUURFeFYwWl
hOMExXVXRhMkZ6ZVM1dFppNW5iM111Y0d3eEtqQW9CZ2txaGtpRzl3MEJDUUVXRzJsdVptOHVaUzFrWld0c1lYSmhZMnBs
UUcxbUxtZHZkaTV3YkRDQ0FTSXdEUVlKS29aSWh2Y05BUUVCQlFBRGdnRVBBRENDQVFvQ2dnRUJBTXZ5VlhHajhZTmh5Nl
AyOGJLajlNbGVBNytRWEtDdFBKWjRNNk1JeGlhcUE0bG9kZDlObytXc2dSRVRWekVQaUI4cmFMOW4zdU0rUkJGd0syQTRW
dnVBV3VHWngyZHJrZk1abnBTVkZMT3NRbmFkQjFyakJDWTVHL3BNWDZlSTdCbHR4NFhGWUsvMWNZMVUrbUZWYzk0UnlmeX
h5eTBaV1NEOElHVjluMEFpbERwUmZJSkJPdTVhM29xdXo4WlpHdVd5VTk1S1dCS1JBRDdTVjJicFRsWVdYNFVIaFRlMzIz
SFRZTDNyRGJLUDczSEFveWxPYlNtU3ZtQjlNeU56V2dCZjczVU9IbXpYUHFwdVJiTEZuUitsbFRBMEZBOGtPeWx4dGlqeW
dNWHBJQ09haTdhdjJvZkd0NjV2MEdKZzV3bEp1cVd2a1FYRlV5b3lHR1VZYVFzQ0F3RUFBYU9CclRDQnFqQWRCZ05WSFE0
RUZnUVV4N3hLajFUWENvck9FeGEyaFkvamR6Nk5rQTB3SHdZRFZSMGpCQmd3Rm9BVUJiK1BhcnRkNlRWNFBWMWtUVXJ0Sm
Fkc1Nkb3dXZ1lJS3dZQkJRVUhBUUVFVGpCTU1Fb0dDQ3NHQVFFRkJ6QUNoajVtYVd4bE9pOHZMeTl6WVhBdGQybHVMVGd5
Tmk5RFpYSjBSVzV5YjJ4c0wzTmhjQzEzYVc0dE9ESTJYMlZMWVhONUxWTjFZa05CS0RFcExtTnlkREFNQmdOVkhSTUJBZj
hFQWpBQU1BMEdDU3FHU0liM0RRRUJEUVVBQTRJQ0FRQ2tkVVIyRGhnaWV4VVcreTJyZ2FFNm9yV0JQeU14dmVIMklQdjBy
UEd6cWRnVUZjTkg4MTZZekRvckVuT0F2YlJMQjhCYW9IK1dnL2VFbEFReHFFNSs0N1ZnU2NJVUY0b05Id1hubmZsUjFYUm
9ZY0ZaL2ZCa0lXMm5mT0sxQzh5MnZIdFpHMVFFeXlWRC9jeHY3dWJnT2lKZk9ZU2NzSHY1REl0U3RGVUJjbHZnM3hyRmky
ekc1YWhibE13cUNHcnZnUEtPeFI5K21YR0QrZW9UaEJIRVA2YUpGM1p1NDFtVndULzRjYlNyNW0zYzc3ZGVFUTJDcFFQR0
w4NzRQaUh5OW9ta2pldjlGNXlvQnpJN3lwaGFseUVJZGJBU1UwVWlVRXJqYlMraG53MFJFclYxYlFRelFmUzdxaUtNQlpU
TTRwek92L1JvNmYrT2NCZjdjMTZYdEhyRWdsaS9hTmFnS28zNG5GaFVzY1FjVVRDaDNNc0NLdVZTWlUzZGJDZFNMSXZkb0
pJUzVGTFArZ3I4TGJRVzl1Ui9OZ3dKaFlyL3cwNms2QU9GK1RhSnc4ZWFrdjVFTERPdXpoaXBxQjYzQnVNU0NHRlpjVVEy
YkRoZGM1Z2NWOUdsTmdWRVhtVG9lZTNmbjg5T1FUQzdHckN3RnpOeHdBTTZnSjBNQVJ5V2w1SG1nci9wT2IxTVg1VmVoZ2
FvSHBqb3ZlTUFhY09OYnRpT3dmTVV5aFBkQ0ptbkxQNjdsb2t2R3E3UERKL0RVYmVzcEFxVm05MVRNNlFiV2pkYW5LR0I2
a0pZKzdINUVTSThzcC9uempIWGRaeGVJUE83bE9USXRLZFJXODJrUmNCUjlUTkRTUzZydDVzSTE2TFcwTkNKMnpwcll0OF
hyTk83MjhsanlBPT0iXX0
```


B.2.3 Pełna postać przykładowych danych komendy przesyłanych do kasy fiskalnej zakodowana w Base64URL:


```
eyJhdHRyaWJ1dGVzIjp7ImNwZFNlcnZpY2VOYW1lIjoiS0ZEIn19
```


B.2.4 Pełna postać przykładowych danych do podpisu komendy przesyłanych do kasy fiskalnej zakodowana w Base64URL:


```
eyJhbGciOiJSUzI1NiIsIng1YyI6WyJNSUlGSERDQ0F3U2dBd0lCQWdJVE9nQUFBQWptajFXQlhVNm1PZ0FCQUFBQUNEQU
5CZ2txaGtpRzl3MEJBUTBGQURBV01SUXdFZ1lEVlFRREV3dGxTMkZ6ZVMxVGRXSkRRVEFnRncweE56QTRNakl3TmpNek1U
TmFHQTh5TURreU1EY3hNREV5TWpjeU9Wb3dnY2d4Q3pBSkJnTlZCQVlUQWxCTU1SUXdFZ1lEVlFRSUV3dE5ZWHB2ZDJsbF
kydHBaVEVSTUE4R0ExVUVCeE1JVjJGeWMzcGhkMkV4SHpBZEJnTlZCQW9NRmsxcGJtbHpkR1Z5YzNSM2J5QkdhVzVoYm5Q
RHMzY3hJekFoQmdOVkJBc1RHa1JsY0dGeWRHRnRaVzUwSUVsdVptOXliV0YwZVhwaFkycHBNUjR3SEFZRFZRUURFeFYwWl
hOMExXVXRhMkZ6ZVM1dFppNW5iM111Y0d3eEtqQW9CZ2txaGtpRzl3MEJDUUVXRzJsdVptOHVaUzFrWld0c1lYSmhZMnBs
```

UUcxbUxtZHZkaTV3YkRDQ0FTSXdEUVlKS29aSWh2Y05BUUVCQlFBRGdnRVBBRENDQVFvQ2dnRUJBTXZ5VlhHajhZTmh5Nl
AyOGJLajlNbGVBNytRWEtDdFBKWjRNNk1JeGlhcUE0bG9kZDlObytXc2dSRVRWekVQaUI4cmFMOW4zdU0rUkJGd0syQTRW
dnVBV3VHWngyZHJrZk1abnBTVkZMT3NRbmFkQjFyakJDWTVHL3BNWDZlSTdCbHR4NFhGWUsvMWNZMVUrbUZWYzk0UnlmeX
h5eTBaV1NEOElHVjluMEFpbERwUmZJSkJPdTVhM29xdXo4WlpHdVd5VTk1S1dCS1JBRDdTVjJicFRsWVdYNFVIaFRlMzIz
SFRZTDNyRGJLUDczSEFveWxPYlNtU3ZtQjlNeU56V2dCZjczVU9IbXpYUHFwdVJiTEZuUitsbFRBMEZBOGtPeWx4dGlqeW
dNWHBJQ09haTdhdjJvZkd0NjV2MEdKZzV3bEp1cVd2a1FYRlV5b3lHR1VZYVFzQ0F3RUFBYU9CclRDQnFqQWRCZ05WSFE0
RUZnUVV4N3hLajFUWENvck9FeGEyaFkvamR6Nk5rQTB3SHdZRFZSMGpCQmd3Rm9BVUJiK1BhcnRkNlRWNFBWMWtUVXJ0Sm
Fkc1Nkb3dXZ1lJS3dZQkJRVUhBUUVFVGpCTU1Fb0dDQ3NHQVFVRkJ6QUNoajVtYVd4bE9pOHZMeTl6WVhBdGQybHVMVGd5
Tmk5RFpYSjBSVzV5YjJ4c0wzTmhjQzEzYVc0dE9ESTJYMlZMWVhONUxWTjFZa05CS0RFcExtTnlkREFNQmdOVkhSTUJBZj
hFQWpBQU1BMEdDU3FHU0liM0RRRUJEUVVBQTRJQ0FRQ2tkVVIyRGhnaWV4VVcreTJyZ2FFNm9yV0JQeU14dmVIMklQdjBy
UEd6cWRnVUZjTkg4MTZZekRvckVuT0F2YlJMQjhCYW9IK1duL2VFbEFReHFFNSs0N1ZnU2NJVUY0b05Id1hubmZsUjFYUm
9ZY0ZaL2ZCa0lXMm5mT0sxQzh5MnZIdFpHMVFFeXlWRC9jeHY3dWJnT2lKZk9ZU2NzSHY1REl0U3RGVUJjbHZnM3hyRmky
ekc1YWhibE13cUNHcnZnUEtPeFI5K21YR0QrZW9UaEJIRVA2YUpGM1p1NDFtVndULzRjYlNyNW0zYzc3ZGVFUTJDcFFQR0
w4NzRQaUh5OW9ta2pldjlGNXlvQnpJN3lwaGFseUVJZGJBU1UwVWlVRXJqYlMraG53MFJFclYxYlFRelFmUzdxaUtNQlpU
TTRwek92L1JvNmYrT2NCZjdjMTZYdEhyRWdsaS9hTmFnS28zNG5GaFVzY1FjVVRDaDNNc0NLdVZTWlUzZGJDZFNMSXZkb0
pJUzVGTFArZ3I4TGJRVzl1Ui9OZ3dKaFlyL3cwNms2QU9GK1RhSnc4ZWFrdjVFTERPdXpoaXBxQjYzQnVNU0NHRlpjVVEy
YkRoZGM1Z2NWOUdsTmdWRVhtVG9lZTNmbjg5T1FUQzdHckN3RnpOeHdBTTZnSjBNQVJ5V2w1SG1nci9wT2IxTVg1VmVoZ2
FvSHBqb3ZlTUFhY09OYnRpT3dmTVV5aFBkQ0ptbkxQNjdsb2t2R3E3UERKL0RVYmVzcEFxVm05MVRNNlFiV2pkYW5LR0I2
a0pZKzdINUVTSThzcC9uempIWGRaeGVJUE83bE9USXRLZFJXODJrUmNCUjlUTkRTUzZydDVzSTE2TFcwTkNKMnpwcll0OF
hyTk83MjhsanlBPT0iXX0.eyJhdHRyaWJ1dGVzIjp7ImNwZFNlcnZpY2VOYW1lIjoiS0ZEIn19

B.2.5 Pełna postać podpisu przykładowej komendy przesyłanej do kasy fiskalnej:

HlKhuau2-ZLYoBip8ed2J7Js5HHOr1b96vlh-udv0OUjm5wWc0wSPCTqDe4rYe9RlqeG8Z4xXbPJE287o01bYtqE-
VuYZL5sDNHvLi1RQBZqTTHpWCNOw3mfM6vrKX_EXJ1wNeGu8aavozYKfVxIHWNZfQz6Ff1dCiAkxxXu35dEyBYGIZHbEz3
4AJu8KOY-
O24ZV6qr2tERB_SUYOgS4ZgigvY9loCDb_Vuui2sKYTMW55bT_BBL0gdm8yp7M2RNNcHitrGgEsen5otmpsgzh-
hQAP7rZYZw05l0gLU8xAaN_2RMIaz1vN1uAM4o8o7mxe-FFv1RLSP1zoMU-NGHw

B.2.6 Pełna postać obiektu JWS przykładowej komendy przesyłanej do kasy fiskalnej:

eyJhbGciOiJSUzI1NiIsIng1YyI6WyJNSUlGSERDQ0F3U2dBd0lCQWdJVE9nQUFBQWptajFXQlhVNm1PZ0FCQUFBQUNEQU
5CZ2txaGtpRzl3MEJBUTBGQURBV01SUXdFZ1lEVlFRREV3dGxTMkZ6ZVMxVGRXSkRRVEFnRncweE56QTRNakl3TmpNek1U
TmFHQTh5TURreU1EY3hNREV5TWpjeU9Wb3dnY2d4Q3pBSkJnTlZCQVlUQWxCTU1SUXdFZ1lEVlFSUV3dE5ZWHB2ZDJsbF
kydHBaVEVSTUE4R0ExVUVCeE1JVjJGeWMzcGhkMkV4SHpBZEJnTlZCQW9NRmsxcGJtbHpkR1Z5YzNSM2J5QkdhVzVoYm5Q
RHMzY3hJekFoQmdOVkJBc1RHa1JsY0dGeWRHRnRaVzUwSUVsdVptOXliV0YwZVhwaFkycHBNUjR3SEFZRFZRUURFeFYwWl
hOMExXVXRhMkZ6ZVM1dFppNW5iM1l1Y0d3eEtqQW9CZ2txaGtpRzl3MEJDUUVXRzJsdVptOHVaUzFrWld0c1lYSmhZMnBs
UUcxbUxtZHZkaTV3YkRDQ0FTSXdEUVlKS29aSWh2Y05BUUVCQlFBRGdnRVBBRENDQVFvQ2dnRUJBTXZ5VlhHajhZTmh5Nl
AyOGJLajlNbGVBNytRWEtDdFBKWjRNNk1JeGlhcUE0bG9kZDlObytXc2dSRVRWekVQaUI4cmFMOW4zdU0rUkJGd0syQTRW
dnVBV3VHWngyZHJrZk1abnBTVkZMT3NRbmFkQjFyakJDWTVHL3BNWDZlSTdCbHR4NFhGWUsvMWNZMVUrbUZWYzk0UnlmeX
h5eTBaV1NEOElHVjluMEFpbERwUmZJSkJPdTVhM29xdXo4WlpHdVd5VTk1S1dCS1JBRDdTVjJicFRsWVdYNFVIaFRlMzIz
SFRZTDNyRGJLUDczSEFveWxPYlNtU3ZtQjlNeU56V2dCZjczVU9IbXpYUHFwdVJiTEZuUitsbFRBMEZBOGtPeWx4dGlqeW
dNWHBJQ09haTdhdjJvZkd0NjV2MEdKZzV3bEp1cVd2a1FYRlV5b3lHR1VZYVFzQ0F3RUFBYU9CclRDQnFqQWRCZ05WSFE0
RUZnUVV4N3hLajFUWENvck9FeGEyaFkvamR6Nk5rQTB3SHdZRFZSMGpCQmd3Rm9BVUJiK1BhcnRkNlRWNFBWMWtUVXJ0Sm
Fkc1Nkb3dXZ1lJS3dZQkJRVUhBUUVFVGpCTU1Fb0dDQ3NHQVFVRkJ6QUNoajVtYVd4bE9pOHZMeTl6WVhBdGQybHVMVGd5
Tmk5RFpYSjBSVzV5YjJ4c0wzTmhjQzEzYVc0dE9ESTJYMlZMWVhONUxWTjFZa05CS0RFcExtTnlkREFNQmdOVkhSTUJBZj
hFQWpBQU1BMEdDU3FHU0liM0RRRUJEUVVBQTRJQ0FRQ2tkVVIyRGhnaWV4VVcreTJyZ2FFNm9yV0JQeU14dmVIMklQdjBy
UEd6cWRnVUZjTkg4MTZZekRvckVuT0F2YlJMQjhCYW9IK1duL2VFbEFReHFFNSs0N1ZnU2NJVUY0b05Id1hubmZsUjFYUm
9ZY0ZaL2ZCa0lXMm5mT0sxQzh5MnZIdFpHMVFFeXlWRC9jeHY3dWJnT2lKZk9ZU2NzSHY1REl0U3RGVUJjbHZnM3hyRmky
ekc1YWhibE13cUNHcnZnUEtPeFI5K21YR0QrZW9UaEJIRVA2YUpGM1p1NDFtVndULzRjYlNyNW0zYzc3ZGVFUTJDcFFQR0
w4NzRQaUh5OW9ta2pldjlGNXlvQnpJN3lwaGFseUVJZGJBU1UwVWlVRXJqYlMraG53MFJFclYxYlFRelFmUzdxaUtNQlpU
TTRwek92L1JvNmYrT2NCZjdjMTZYdEhyRWdsaS9hTmFnS28zNG5GaFVzY1FjVVRDaDNNc0NLdVZTWlUzZGJDZFNMSXZkb0
pJUzVGTFArZ3I4TGJRVzl1Ui9OZ3dKaFlyL3cwNms2QU9GK1RhSnc4ZWFrdjVFTERPdXpoaXBxQjYzQnVNU0NHRlpjVVEy
YkRoZGM1Z2NWOUdsTmdWRVhtVG9lZTNmbjg5T1FUQzdHckN3RnpOeHdBTTZnSjBNQVJ5V2w1SG1nci9wT2IxTVg1VmVoZ2
FvSHBqb3ZlTUFhY09OYnRpT3dmTVV5aFBkQ0ptbkxQNjdsb2t2R3E3UERKL0RVYmVzcEFxVm05MVRNNlFiV2pkYW5LR0I2
a0pZKzdINUVTSThzcC9uempIWGRaeGVJUE83bE9USXRLZFJXODJrUmNCUjlUTkRTUzZydDVzSTE2TFcwTkNKMnpwcll0OF
hyTk83MjhsanlBPT0iXX0.eyJhdHRyaWJ1dGVzIjp7ImNwZFNlcnZpY2VOYW1lIjoiS0ZEIn19.HlKhuau2-
ZLYoBip8ed2J7Js5HHOr1b96vlh-udv0OUjm5wWc0wSPCTqDe4rYe9RlqeG8Z4xXbPJE287o01bYtqE-
VuYZL5sDNHvLi1RQBZqTTHpWCNOw3mfM6vrKX_EXJ1wNeGu8aavozYKfVxIHWNZfQz6Ff1dCiAkxxXu35dEyBYGIZHbEz3
4AJu8KOY-
O24ZV6qr2tERB_SUYOgS4ZgigvY9loCDb_Vuui2sKYTMW55bT_BBL0gdm8yp7M2RNNcHitrGgEsen5otmpsgzh-
hQAP7rZYZw05l0gLU8xAaN_2RMIaz1vN1uAM4o8o7mxe-FFv1RLSP1zoMU-NGHw

B.3 Przykładowe dane procesu szyfrowania komendy w środowisku testowym

B.3.1 Pełna postać chronionego nagłówka obiektu JWE komend przesyłanych do kasy:

{"enc":"A128CBC-HS256","alg":"RSA1_5","kid":"cc82d4ae40f68aa342c42d59ac6ed404,CN=MF e-Kasy"}

B.3.2 Pełna postać chronionego nagłówka obiektu JWE komend przesyłanych do kasy fiskalnej zakodowana w Base64URL:

eyJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiUlNBMV81Iiwia2lkIjoiY2M4MmQ0YWU0MGY2OGFhMzQyYzQyZDU5YWM2ZWQ0MDQsQ049TUYgZS1LYXN5In0

B.3.3 Wartości przykładowych danych użytych do szyfrowania zakodowanych szesnastkowo:

JWE_AES_CEK => 852cde285e375dac45ff7c44ee6d12e306b4e7086a2e0f3e0dbc1e3e1e3a0e68

JWE_MAC_KEY => 852cde285e375dac45ff7c44ee6d12e3
JWE_AES_KEY => 06b4e7086a2e0f3e0dbc1e3e1e3a0e68

JWE_AES_IV => 9641366ce173224c452a914e6de088c3

B.3.4 Zaszyfrowana wartość przykładowego klucza algorytmu szyfrującego algorytmem asymetrycznym RSA z wykorzystaniem klucza publicznego kasy zakodowana w Base64URL:

hsileeNCtbhjLR60diiBZ7U6kFPqzU3Pc6DDneWQncob1sZTEv7bsqlAv-QDmR3liTRWuOzcYgduuDwAbmz1xwFI3cVObVeQBiRAgBtFuX_xEpmBdXAzXrMXY37dX1SoCu0Rno0HnBs5bDsnuX4TiZe4jEKNggOhpf88mErGW26BwU1WbvFlyj9HhEfI2H46D-y29djnkXI_7MpM994hTRTq6JGPE-9m2ZjOtU6Yw4Ty1kRmUeK9iWQkdIKJHy6TGHD9qnh03Odcyu_DPHJnbmhhB5AaT5yAD9kGcitcMC4PUDju3_qcHgiwPo94s4m8j1RBo7M8jldVJvvOpU28ng

B.3.5 Przykładowa wartość wektora inicjującego zakodowana w Base64URL:

lkE2bOFzIkxFKpFObeCIww

B.3.6 Przykładowa wartość zaszyfrowanych danych zakodowana w Base64URL:

PoikvBdxUJgfLYAr9tyYOediKO7oQTdEUAPcW6QSKcmPCu1e3TKtk-ypKVXtMrJvJd0uRweKpGvx_uyU-IEENg_Dh4o1Q8A7PQ5D2of_qZCW9pXi-DCnSE6wtPAqgUCYKbeXWdJj8S-jzDrx6z-nu9ie25f4pw5EnRsA7pGLfk0MIao6oaEDcrmVm646tf9ezCKwACZX3HyOLpN0Q6PtovXPriGV07V7bQ-MCSsj0AoxKMdjv1YNUGblU-WxAPaSki-7L54YgkMR3ob9eRUZNAHIzs2jNTAPCuOML2zycO4Qz0saa5h4Q8zuG9WOOaAKJI0CQqHWh3FRqMSOINoXkbay5QVzrZ-Kbbyf6LusspxI5aibMNPBucrXkodWWszFc3th_jPQ4r6YZB-RzAO_inRNQqFsTJneP0OJjkd_0SfkanIcU5sjxsbBH9G6Vry5ECtOr5Me3IPcPIXGcdGqBO3TaklpXCHj1-qOVWeDbZY5xxcQfhhSvYfOtM5ei4yIkNrXIcWTagie-kmlBnF2mtjm0iv1YCuca8a44RcD5BdpaGOr1lEeizjAPBYi8QWtXSU5KDNXeC0gN4zUNPuccuzPzPk1QaQ7Mt8h9rgzOB9cDIoOVLFe_hqAq4fn4xG25QKiTVLcOd8PKB8oA4S_f_4nO6cO7zPx_DP4Tu9cBE4M7DJxjZY2d4A21w-HGx4YukTwaX_w9bcfhKSYNkFYKky6aal80Z4JaMW902NHhleG0ER6c3Y7JFVCyWw9CXIJKfT6BVY8q5CdVFrW4_CF38-AIuXKRU-HizqOjM8TrOErY0hOu5443u7KQedT4pyZWyAzVai4MK1Kj5jLUyLOZ4inHPgqTdT3AaTFX5FDwOM_ivUjbwoptwk7MC8euoHTXQj02yB4p-TpdGsx4qO9BHUg3fgFPNbrSFDWn80KNV8C6VmOBaTNZ8MTLkSB3lQhMEC3mYCeB3fMiy_E79NmePsttGKCcCPotwFv4-qW-cGp11-T_Z5P8_EqN6ss04O0w4PlAq7Q0mJdmpaf0KqnT-gF7KcwYG5Vq3_5DJCXBu0DSigydQyBUl5E4OUH8X02sSNGetmiLuAMkrOV6dysu0bJVlu81OeyN1bQv7cN_qiL1DQBt_gsquhspxI8h1lMHyxQ2ygIrDm-UsMWdjl20jBIy7zlFOVHJxbdna_fZNldA1Tkg1L-vuHdJprEqcBpnjoOKe8wWpGwalreKi4DHOf3nOm_JEfpdxhO7DfPpG6fx-krxkkF2_ybyg773NSATjBBOeRbZo1GrI8Ic7fdHIpFYyxhcCU9zLRJlWg0pjzHJIxoX-prwhW90BHqjFYpnOynMEvs6SXCES4OPFS2mXw8PFr51PkRkYfkSewraTnWwnw3WFqfiOBjCKeDpfbF5axbhT-rg5BTHUi-VvPT3MrPInRy-p0BijKLB9y8Z0R8DLX07ZoWAjJOS55XWdZ8hdPWCoC5O9odTRcUUEvi-uqWQJMQCmZCiRwhsU9vO51T2t-aaWhLL9Q-e58M_pbM0HfLU_ea8jf5Vaf_bXht18BgZi2dvt-vddwY09kVB-jQkzJmvLe2_hcWlrKQ2X7-EmDlLt7iad7Nn20861a2lDKdQjbVDXbXZVF2cp9jdtg_Ls5rMHgcTU2ORJG4jzcHCJi4qRVUsa9t4znWEbtgLS64T64qScxqgcNL8gRzFwLxCCG_6UqFbUgqIkHfWjlzw572rA_WJGB0UVBPiRxltRzHKC2bhc85KTKsvO0qIHVk1DCrF47rTZ-Dx54IzGhsW_BRc5azlcshoNaABAUw2V_hS-

```
DoMsLLpli5qfiRBw_WrhBbZjSFUn1AIL12CeeJss9pZ9ZNe2aPWjd75vTknxURE9mT8-jh1v3DjTs8_eBQWBT9-
BdEy0AEPfKTZgZ4QHxLj_v3VLr3F99Fu2dj977LJ1SiOnXMJlZLhypPrTnwjFuPavNe8HmsvjgysyMgHt_Lu_bx4OQk0P-
MrfwbOXsSjjJivyjS-
P5g2p194L5sGonvh2Jrl5Q_aBHgKIiyakYxEY3zbYcJfS1RoV5MSg2P_MJYoJI1Ffm_AAqUcRBK1dYQLhTIilQzjOb5_TZ
8_3za2pjH7xLWC91egX6d8tFqpyX1XaLchQUObnKJgqubHejatfBZU1BM82BmyigS8PseeDPC2Cj6tg34BKra7q3I20H5X
QrDFbyho7HOlY55jb5UvLsSmHdIAgoFOh7iSnki4iYrkQrPVCWlvbb2KvhNHotCeYFsdxfLa43y21STuYBoNP5Buu-
cz4jovMwQyMZSgU7ojx8ae2RkrGzJxD7p943U9w21mTNJDDBpIdUg_QaPEi9PaxH-7mB72waZfDtNEB5S-
MBQpIdIazD6QB4skD3b2h49rXggBYjyT59yxPrHkhDy_bo352BMqRxokfjZ1KdirVHS4cLy0SXty06E3TCUt5_tFJ-0bo-
kT-Dj4wR7k04Yzd6thPKi6AQJKPZz1ARZEguGu2-9p46AVZd1mCWDTCNlEDsL_gvb7GJFIknZt215voxI6WMjzyLio-
jyGGMBHgoQSsd246LQY-LNJCKJa8a18MbNqpRRBZBdmPnvWUoK8eTQ6NkT3mZQNQcrqvrRtrQ_OECAScwcDoSct4d6C-
_w-
I77E_FNVEvdnVDbWMKJMc9_F99qfBTYPL9AL_Cx89SyoJOrBWiWLClGoPjw91MV3K5fxX_1EXapNyrfWW3jo9OjeVKr42h
eWacLTFMCCdNXYMuwVT8NttBRpkJwee-
dae0vqomtHQQa1_gyqc01J95pAbATYkjAGKYfnImS6c4fEP2VD6EAro7WQzmM3IzEvFF9dWMD5RnuwMKB2HECCxvSKkc03
fQC_xMu0EgliqkE_QyT2aJpPTyf7pB-
zSy2C6gYt5DVlnc8ea6i1ElPSwdaS9uzMVHE0Hqrfq6Px23uZXcBVYcNiSXCguUaAyLmOf6YsXK7hHHx_uoVLVlB3SDME4
GDI8bp0PisW_LTViALvjktsrm0021PqCu58mHqEP9h0jM-s582vcw9orSdi63q2OvK6dBojawORWZ_t-MWTc7r0-
y_766bekLrktyVHJkfbUFM4keDOEP9I4MO9mKHnCLGCmFok5zlJDxtn71M_HXXpwJJ4hrCJIUOT2ZO0glIRGE1YhMqILfh
DJNELhh1ytsqSy32RTOz1qbIog1TilpQOwxbGPUVazwcXTXOFtHrd6O74gpGHQkhWurIcYxLcm4rD8gja97iLm2J2keD5b
HbgCryyjB8BotGZTA_oj1VihMe9P6k69QwUCOo-MgQSVYgq6IXS3EbfdOBbWObjRtytaY46YXY9-4OREk6BlHes8Xn5bG-
O7w0xJ4OKyKAEs6iyRyFktr_RP6rBMOfpOLz90G68hX8ZwOVGWUIE8e8J5gB3XbpPYbX5lWi2kx-
7CYXRDdbYUi36l338tHks-aXcZ8Hb7h-D8bGxObateUSBR3Ka-
6gCDMYHdSYijxHhhBxTTyrAcgzrLKD7CvV4PwQ5cUVx1qE7VeosUMIS9BotMXQmr12C0k1ulAHW8JspE43Mpced0NuUUaX
ib9EVuNKxK1DjLXwtv8OMsugQ4_bOWQMMCpz-
l5o5ciPGht0YkDAZJoODYMDpmZvMJLYb3QBzBbt2kgaG8Si0a_9NZrkpTLOuRM
```

B.3.7a Przykładowa wartość dodatkowych danych uwierzytelniających - nagłówek JWE:

```
eyJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiUlNBMV81Iiwia2lkIjoiY2M4MmQ0YWU0MGY2OGFhMzQyYzQyZDU5YW
M2ZWQ0MDQsQ049TUYgZS1LYXN5In0
```

odzwierciedlenie AAD w postaci szesnastkowej:

```
65794a6c626d4d694f694a424d54493451304a444c5568544d6a5532496977695957786e496a6f69556c4e424d5638
314969776961326c6b496a6f6959324d344d6d5130595755304d4759324f4746684d7a5179597a51795a4455355957
4d325a5751304d4451735130343954555967 5a53314c59584e35496e30
```

B.3.7b Przykład wyliczenia reprezentacji wartości długości dodatkowych danych uwierzytelniających zakodowana w Base64URL:

```
JWE_AAD_URL BYTES LENGTH -> 123

JWE_AAD_URL BITS LENGTH -> 123 * 8 = 984

JWE_AT = [0, 0, 0, 0, 0, 0, 3, 216]
```

odzwierciedlenie w postaci szesnastkowej:

```
00000000000003d8
```

B.3.8a Przykładowa wartość etykiety uwierzytelniającej zakodowana w Base64URL:

```
ct35FpBFiOdWQ7aw8Jk45A
```

odzwierciedlenie w postaci szesnastkowej:

```
72ddf916904588e75643b6b0f09938e4
```

B.3.8b Przykład wyliczenia wartości etykiety uwierzytelniającej przykładowych danych:

Postać szesnastkowa odszyfrowanego 32 bajtowego klucza CEK (Content Encryption Key) B.3.3:

```
852cde285e375dac45ff7c44ee6d12e306b4e7086a2e0f3e0dbc1e3e1e3a0e68
```

pierwsze 16 bajtów wykorzystywane jako klucz w funkcji HMAC (JWE_MAC_KEY):

postać szesnastkowa wykorzystana w funkcji HMAC:
852cde285e375dac45ff7c44ee6d12e3

użyte dane autoryzujące AAD (nagłówek JWE) B.3.7a:

postać ASCII:
{"enc":"A128CBC-HS256","alg":"RSA1_5","kid":"cc82d4ae40f68aa342c42d59ac6ed404,CN=MF e-Kasy"}

postać Base64URL:
eyJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiUlNBMV81Iiwia2lkIjoiY2M4MmQ0YWU0MGY2OGFhMzQyYzQyZDU5YWM2ZWQ0MDQsQ049TUYgZS1LYXN5In0

postać szesnastkowa (bajty postaci Base64URL) wykorzystana w funkcji HMAC:
**65794a6c626d4d694f694a424d54493451304a444c5568544d6a5532496977695957786e496a6f69556c4e424d5638314969776961326c6b496a6f6959324d344d6d5130595755304d4759324f4746684d7a5179597a51795a4455355957
4d325a5751304d4451735130343954555967 5a53314c59584e35496e30**

użyty 16 bajtowy wektor inicjujący IV B.3.5:

postać Base64URL:
lkE2bOFzIkxFKpFObeCIww

postać szesnastkowa wykorzystana w funkcji HMAC:
9641366ce173224c452a914e6de088c3

zaszyfrowane dane użyte do wyliczenia etykiety uwierzytelniającej B.3.6:

postać Base64URL:
PoikvBdxUJgfLYAr9tyYOediKO7oQTdEUAPcW6QSKcmPCu1e3TKtk-ypKVXtMrJvJd0uRweKpGvx_uyU-
IEENg_Dh4o1Q8A7PQ5D2of_qZCW9pXi-DCnSE6wtPAqgUCYKbeXWdJj8S-jzDrx6z-
nu9ie25f4pw5EnRsA7pGLfk0MIao6oaEDcrmVm646tf9ezCKwACZX3HyOLpN0Q6PtovXPriGV07V7bQ-
MCSsj0AoxKMdjv1YNUGblU-WxAPaSki-
7L54YgkMR3ob9eRUZNAHIzs2jNTAPCuOML2zycO4Qz0saa5h4Q8zuG9WOOaAKJI0CQqHWh3FRqMSOINoXkbay5QVzrZ-
Kbbyf6LusspxI5aibMNPBucrXkodWWszFc3th_jPQ4r6YZB-
RzAO_inRNQqFsTJneP0OJjkd_0SfkanIcU5sjxsbBH9G6Vry5ECtOr5Me3IPcPIXGcdGqBO3TaklpXCHj1-
qOVWeDbZY5xxcQfhhSvYfOtM5ei4yIkNrXIcWTagie-
kmlBnF2mtjm0iv1YCuca8a44RcD5BdpaGOr1lEeizjAPBYi8QWtXSU5KDNXeC0gN4zUNPuccuzPzPk1QaQ7Mt8h9rgzOB9
cDIoOVLFe_hqAq4fn4xG25QKiTVLcOd8PKB8oA4S_f_4nO6cO7zPx_DP4Tu9cBE4M7DJxjZY2d4A21w-
HGx4YukTwaX_w9bcfhKSYNkFYKky6aal80Z4JaMW902NHhleG0ER6c3Y7JFVCyWw9CXIJKfT6BVY8q5CdVFrW4_CF38-
AIuXKRU-
HizqOjM8TrOErY0hOu5443u7KQedT4pyZWyAzVai4MK1Kj5jLUyLOZ4inHPgqTdT3AaTFX5FDwOM_ivUjbwoptwk7MC8eu
oHTXQj02yB4p-
TpdGsx4qO9BHUg3fgFPNbrSFDWn80KNV8C6VmOBaTNZ8MTLkSB3lQhMEC3mYCeB3fMiy_E79NmePsttGKCcCPotwFv4-
qW-cGp11-T_Z5P8_EqN6ss04O0w4PlAq7Q0mJdmpaf0KqnT-
gF7KcwYG5Vq3_5DJCXBu0DSigydQyBUl5E4OUH8X02sSNGetmiLuAMkrOV6dysu0bJVlu81OeyN1bQv7cN_qiL1DQBt_gs
quhspxI8h1lMHyxQ2ygIrDm-UsMWdjl20jBIy7zlFOVHJxbdna_fZNldA1Tkg1L-
vuHdJprEqcBpnjoOKe8wWpGwalreKi4DHOf3nOm_JEfpdxhO7DfPpG6fx-
krxkkF2_ybyg773NSATjBBOeRbZo1GrI8Ic7fdHIpFYyxhcCU9zLRJlWg0pjzHJIxoX-
prwhW90BHqjFYpnOynMEvs6SXCES4OPFS2mXw8PFr51PkRkYfkSewraTnWwnw3WFqfiOBjCKeDpfbF5axbhT-rg5BTHUi-
VvPT3MrPInRy-p0BijKLB9y8Z0R8DLX07ZoWAjJOS55XWdZ8hdPWCoC5O9odTRcUUEvi-
uqWQJMQCmZCiRwhsU9vO51T2t-aaWhLL9Q-e58M_pbM0HfLU_ea8jf5Vaf_bXht18BgZi2dvt-vddwY09kVB-
jQkzJmvLe2_hcWlrKQ2X7-
EmDlLt7iad7Nn20861a2lDKdQjbVDXbXZVF2cp9jdtg_Ls5rMHgcTU2ORJG4jzcHCJi4qRVUsa9t4znWEbtgLS64T64qSc
xqgcNL8gRzFwLxCCG_6UqFbUgqIkHfWjlzw572rA_WJGB0UVBPiRxltRzHKC2bhc85KTKsvO0qIHVk1DCrF47rTZ-
Dx54IzGhsW_BRc5azlcshoNaABAUw2V_hS-
DoMsLLpli5qfiRBw_WrhBbZjSFUn1AIL12CeeJss9pZ9ZNe2aPWjd75vTknxURE9mT8-jh1v3DjTs8_eBQWBT9-
BdEy0AEPfKTZgZ4QHxLj_v3VLr3F99Fu2dj977LJ1SiOnXMJlZLhypPrTnwjFuPavNe8HmsvjgysyMgHt_Lu_bx4OQk0P-
MrfwbOXsSjjJivyjS-
P5g2p194L5sGonvh2Jrl5Q_aBHgKIiyakYxEY3zbYcJfS1RoV5MSg2P_MJYoJI1Ffm_AAqUcRBK1dYQLhTIilQzjOb5_TZ
8_3za2pjH7xLWC91egX6d8tFqpyX1XaLchQUObnKJgqubHejatfBZU1BM82BmyigS8PseeDPC2Cj6tg34BKra7q3I20H5X
QrDFbyho7HOlY55jb5UvLsSmHdIAgoFOh7iSnki4iYrkQrPVCWlvbb2KvhNHotCeYFsdxfLa43y21STuYBoNP5Buu-
cz4jovMwQyMZSgU7ojx8ae2RkrGzJxD7p943U9w21mTNJDDBpIdUg_QaPEi9PaxH-7mB72waZfDtNEB5S-
MBQpIdIazD6QB4skD3b2h49rXggBYjyT59yxPrHkhDy_bo352BMqRxokfjZ1KdirVHS4cLy0SXty06E3TCUt5_tFJ-0bo-
kT-Dj4wR7k04Yzd6thPKi6AQJKPZz1ARZEguGu2-9p46AVZd1mCWDTCNlEDsL_gvb7GJFIknZt215voxI6WMjzyLio-
jyGGMBHgoQSsd246LQY-LNJCKJa8a18MbNqpRRBZBdmPnvWUoK8eTQ6NkT3mZQNQcrqvrRtrQ_OECAScwcDoSct4d6C-
_w-

I77E_FNVEvdnVDbWMKJMc9_F99qfBTYPL9AL_Cx89SyoJOrBWiWLClGoPjw91MV3K5fxX_1EXapNyrfWW3jo9OjeVKr42h
eWacLTFMCCdNXYMuwVT8NttBRpkJwee-
dae0vqomtHQQa1_gyqc01J95pAbATYkjAGKYfnImS6c4fEP2VD6EAro7WQzmM3IzEvFF9dWMD5RnuwMKB2HECCxvSKkc03
fQC_xMu0Eg1iqkE_QyT2aJpPTyf7pB-
zSy2C6gYt5DVlnc8ea6i1ElPSwdaS9uzMVHE0Hqrfq6Px23uZXcBVYcNiSXCguUaAyLmOf6YsXK7hHHx_uoVLVlB3SDME4
GDI8bp0PisW_LTViALvjktsrm0021PqCu58mHqEP9h0jM-s582vcw9orSdi63q2OvK6dBojawORWZ_t-MWTc7r0-
y_766bekLrktyVHJkfbUFM4keDOEP9I4MO9mKHnCLGCmFok5zlJDxtn71M_HXXpwJJ4hrCJIUOT2ZO0glIRGE1YhMqILfh
DJNELhh1ytsqSy32RTOz1qbIog1TilpQOwxbGPUVazwcXTXOFtHrd6O74gpGHQkhWurIcYxLcm4rD8gja97iLm2J2keD5b
HbgCryyjB8BotGZTA_oj1VihMe9P6k69QwUCOo-MgQSVYgq6IXS3EbfdOBbWObjRtytaY46YXY9-4OREk6BlHes8Xn5bG-
O7w0xJ4OKyKAEs6iyRyFktr_RP6rBMOfpOLz90G68hX8ZwOVGWUIE8e8J5gB3XbpPYbX5lWi2kx-
7CYXRDdbYUi361338tHks-aXcZ8Hb7h-D8bGxObateUSBR3Ka-
6gCDMYHdSYijxHhhBxTTyrAcgzrLKD7CvV4PwQ5cUVx1qE7VeosUMIS9BotMXQmr12C0k1ulAHW8JspE43Mpced0NuUUaX
ib9EVuNKxK1DjLXwtv8OMsugQ4_bOWQMMCpz-
l5o5ciPGht0YkDAZJoODYMDpmZvMJLYb3QBzBbt2kgaG8Si0a_9NZrkpTLOuRM

postać szesnastkowa wykorzystana w funkcji HMAC:
**3e88a4bc177150981f2d802bf6dc9839e76228eee84137445003dc5ba41229c98f0aed5edd32ad93eca92955ed32b2
6f25dd2e47078aa46bf1feec94f88104360fc3878a3543c03b3d0e43da87ffa99096f695e2f830a7484eb0b4f02a81
409829b79759d263f12fa3cc3af1eb3fa7bbd89edb97f8a70e449d1b00ee918b7e4d0c21aa3aa1a10372b9959bae3a
b5ff5ecc22b0002657dc7c8e2e937443a3eda2f5cfae2195d3b57b6d0f8c092b23d00a3128c763bf560d5066e553e5
b100f692922fbb2f9e18824311de86fd7915193401c8cecda335300f0ae38c2f6cf270ee10cf4b1a6b987843ccee1b
d58e39a00a248d0242a1d6877151a8c48e20da1791b6b2e50573ad9f8a6dbc9fe8bbacb29c48e5a89b30d3c1b9cad7
9287565accc5737b61fe33d0e2be98641f91cc03bf8a744d42a16c4c99de3f43898e477fd127e46a721c539b23c6c6
c11fd1ba56bcb9102b4eaf931edc83dc3c85c671d1aa04edd36a49695c21e3d7ea8e5567836d9639c717107e1852bd
87ceb4ce5e8b8c8890dad721c5936a089efa49a50671769ad8e6d22bf5602b9c6bc6b8e11703e417696863abd6511e
8b38c03c1622f105ad5d2539283357782d20378cd434fb9c72eccfccf93541a43b32df21f6b833381f5c0c8a0e54b1
5efe1a80ab87e7e311b6e502a24d52dc39df0f281f280384bf7ffe273ba70eef33f1fc33f84eef5c044e0cec32718d
9636778036d70f871b1e18ba44f0697ff0f5b71f84a4983641582a4cba69a97cd19e0968c5bdd36347865786d0447a
73763b245542c96c3d09720929f4fa05563cab909d545ad6e3f085dfcf8022e5ca454f878b3a8e8ccf13ace12b6348
4ebb9e38deeeca41e753e29c995b203355a8b830ad4a8f98cb5322ce6788a71cf82a4dd4f701a4c55f9143c0e33f8a
f5236f0a29b7093b302f1eba81d35d08f4db2078a7e4e9746b31e2a3bd047520ddf8053cd6eb4850d69fcd0a355f02
e9598e05a4cd67c3132e4481de54213040b799809e0777cc8b2fc4efd36678fb2db462827023e8b7016fe3ea96f9c1
a9d75f93fd9e4ff3f12a37ab2cd383b4c383e502aed0d2625d9a969fd0aaa74fe805eca730606e55ab7ff90c909706
ed034a2832750c81525e44e0e507f17d36b123467ad9a22ee00c92b395e9dcacbb46c9565bbcd4e7b23756d0bfb70d
fea88bd43401b7f82caae86ca7123c87594c1f2c50db2808ac39be52c316763976d23048cbbce514e5472716dd9daf
df64d95d0354e48352febee1dd269ac4a9c0699e3a0e29ef305a91b06a5ade2a2e031ce7f79ce9bf2447e977184eec
37cfa46e9fc7e92bc64905dbfc9bca0efbdcd4804e304139e45b668d46ac8f0873b7dd1c8a45632c6170253dccb449
956834a63cc7248c685fea6bc215bdd011ea8c56299ceca7304bece925c2112e0e3c54b6997c3c3c5af9d4f9119187
e449ec2b6939d6c27c37585a9f88e06308a783a5f6c5e5ac5b853fab8390531d48be56f3d3dccacf227472fa9d018a
328b07dcbc67447c0cb5f4ed9a1602324e4b9e5759d67c85d3d60a80b93bda1d4d1714504be2faea964093100a6642
891c21b14f6f3b9d53dadf9a69684b2fd43e7b9f0cfe96ccd077cb53f79af237f955a7ff6d786dd7c060662d9dbedf
af75dc18d3d91507e8d0933266bcb7b6fe171696b290d97efe1260e52edee269decd9f6d3ceb56b694329d4236d50d
76d7655176729f6376d83f2ece6b30781c4d4d8e4491b88f37070898b8a91554b1af6de339d611bb602d2eb84fae2a
49cc6a81c34bf204731702f10821bfe94a856d482a2241df5a3973c39ef6ac0fd624607451504f891c65b51cc7282d
9b85cf392932acbced2a207564d430ab178eeb4d9f83c79e08cc686c5bf0517396b395cb21a0d680040530d95fe14b
e0e832c2cba658b9a9f891070fd6ae105b663485527d4020bd7609e789b2cf6967d64d7b668f5a377be6f4e49f1511
13d993f3e8e1d6fdc38d3b3cfde0505814fdf81744cb40043df293660678407c4b8ffbf754baf717df45bb6763f7be
cb2754a23a75cc26564b872a4fad39f08c5b8f6af35ef079acbe3832b323201edfcbbbf6f1e0e424d0ff8cadfc1b39
7b128e3262bf28d2f8fe60da9d7de0be6c1a89ef87626b97943f6811e02888b26a4631118df36d87097d2d51a15e4c
4a0d8ffcc258a0923515f9bf000a9471104ad5d6102e14c88a54338ce6f9fd367cff7cdada98c7ef12d60bdd5e817e
9df2d16aa725f55da2dc85050e6e728982ab9b1de8dab5f05953504cf36066ca2812f0fb1e7833c2d828fab60df804
aadaeeadc8db41f95d0ac315bca1a3b1ce958e798dbe54bcbb12987748020a053a1ee24a7922e2262b910acf5425a5
bdb6f62af84d1e8b4279816c7717cb6b8df2db5493b9806834fe41baef9ccf88e8bccc10c8c652814ee88f1f1a7b64
64ac6cc9c43ee9f78dd4f70db59933490c306921d520fd068f122f4f6b11feee607bdb06997c3b4d101e52f8c050a4
87486b30fa401e2c903ddbda1e3dad78200588f24f9f72c4fac79210f2fdba37e7604ca91c6891f8d9d4a762ad51d2
e1c2f2d125edcb4e84dd3094b79fed149fb46e8fa44fe0e3e3047b934e18cddead84f2a2e8040928f673d40459120b
86bb6fbda78e805597759825834c2365103b0bfe0bdbec62452249d9b76d79be8c48e96323cf22e2a3e8f21863011e
0a104ac776e3a2d063e2cd2422896bc6b5f0c6cdaa945105905d98f9ef594a0af1e4d0e8d913de665035072baafad1
b6b43f38408049cc1c0e849cb7877a0beff0f88efb13f14d544bdd9d50db58c28931cf7f17df6a7c14d83cbf402ff0
b1f3d4b2a093ab0568962c2946a0f8f0f75315dcae5fc57ff51176a9372adf596de3a3d3a37952abe3685e59a70b4c
530209d35760cbb0553f0db6d051a6427079ef9d69ed2faa89ad1d041ad7f832a9cd3527de6901b0136248c018a61f
9c8992e9ce1f10fd950fa100ae8ed643398cdc8cc4bc517d756303e519eec0c281d871020b1bd22a4734ddf402ff13
2ed048358aa904fd0c93d9a2693d3c9fee907ecd2cb60ba818b790d596773c79aea2d4494f4b075a4bdbb33151c4d0
7aab7eae8fc76dee65770155870d8925c282e51a0322e639fe98b172bb8471f1feea152d5941dd20cc13818323c6e9
d0f8ac5bf2d356200bbe392db2b9b4d36d4fa82bb9f261ea10ff61d2333eb39f36bdcc3da2b49d8badead8ebcae9d0
688dac0e45667fb7e3164dceebd3ecbfefae9b7a42eb92dc951c991f6d414ce247833843fd23830ef662879c22c60a
6168939ce5243c6d9fbd4cfc75d7a70249e21ac224850e4f664ed20948446135621 32a20b7e10c93442e1875cadb2a
4b2df64533b3d6a6c8a20d538a5a503b0c5b18f5156b3c1c5d35ce16d1eb77a3bbe20a461d09215aeac8718c4b726e
2b0fc8236bdee22e6d89da4783e5b1db802af2ca307c068b4665303fa23d558a131ef4fea4ebd4305023a8f8c81049
5620aba2174b711b7dd3816d639b8d1b72b5a638e985d8f7ee0e44493a0651deb3c5e7e5b1be3bbc34c49e0e2b2280
12cea2c91c8592daff44feab04c39fa4e2f3f741baf215fc67039519650813c7bc279801dd76e93d86d7e655a2da4c**

7eec261744375b6148b7ea5df7f2d1e4b3e697719f076fb87e0fc6c6c4e6dab5e512051dca6beea00833181dd4988a3c478610714d3cab01c833acb283ec2bd5e0fc10e5c515c75a84ed57a8b143084bd068b4c5d09abd760b4935ba50075bc26ca44e3732971e77436e51469789bf4456e34ac4ad438cb5f0b6ff0e32cba0438fdb39640c302a73fa5e68e5c88f1a1b746240c0649a0e0d8303a6666f3092d86f7401cc16edda481a1bc4a2d1affd359ae4a532ceb913

długość dodatkowych danych autoryzujących w formacie Base64URL wynosi 123 bajty, czyli 984 bity i w formacie Big-Endian w postaci szesnastkowej ma wartość B.3.7b:

00000000000003d8

Dokonując konkatenacji bajtowej AAD, IV oraz danych zaszyfrowanych i długości AAD do wyliczenia MAC będzie wykorzystany ciąg bajtów w postaci szesnastkowej:

65794a6c626d4d694f694a424d54493451304a444c5568544d6a5532496977695957786e496a6f69556c4e424d5638
314969776961326c6b496a6f6959324d344d6d5130595755304d4759324f4746684d7a5179597a51795a4455355957
4d325a5751304d4451735130343954555967 5a53314c59584e35496e309641366ce173224c452a914e6de088c33e88
a4bc177150981f2d802bf6dc9839e76228eee84137445003dc5ba41229c98f0aed5edd32ad93eca92955ed32b26f25
dd2e47078aa46bf1feec94f88104360fc3878a3543c03b3d0e43da87ffa99096f695e2f830a7484eb0b4f02a814098
29b79759d263f12fa3cc3af1eb3fa7bbd89edb97f8a70e449d1b00ee918b7e4d0c21aa3aa1a10372b9959bae3ab5ff
5ecc22b0002657dc7c8e2e937443a3eda2f5cfae2195d3b57b6d0f8c092b23d00a3128c763bf560d5066e553e5b100
f692922fbb2f9e18824311de86fd7915193401c8cecda335300f0ae38c2f6cf270ee10cf4b1a6b987843ccee1bd58e
39a00a248d0242a1d6877151a8c48e20da1791b6b2e50573ad9f8a6dbc9fe8bbacb29c48e5a89b30d3c1b9cad79287
565accc5737b61fe33d0e2be98641f91cc03bf8a744d42a16c4c99de3f43898e477fd127e46a721c539b23c6c6c11f
d1ba56bcb9102b4eaf931edc83dc3c85c671d1aa04edd36a49695c21e3d7ea8e5567836d9639c717107e1852bd87ce
b4ce5e8b8c8890dad721c5936a089efa49a50671769ad8e6d22bf5602b9c6bc6b8e11703e417696863abd6511e8b38
c03c1622f105ad5d2539283357782d20378cd434fb9c72eccfccf93541a43b32df21f6b833381f5c0c8a0e54b15efe
1a80ab87e7e311b6e502a24d52dc39df0f281f280384bf7ffe273ba70eef33f1fc33f84eef5c044e0cec32718d9636
778036d70f871b1e18ba44f0697ff0f5b71f84a4983641582a4cba69a97cd19e0968c5bdd36347865786d0447a7376
3b245542c96c3d09720929f4fa05563cab909d545ad6e3f085dfcf8022e5ca454f878b3a8e8ccf13ace12b63484ebb
9e38deeeca41e753e29c995b203355a8b830ad4a8f98cb5322ce6788a71cf82a4dd4f701a4c55f9143c0e33f8af523
6f0a29b7093b302f1eba81d35d08f4db2078a7e4e9746b31e2a3bd047520ddf8053cd6eb4850d69fcd0a355f02e959
8e05a4cd67c3132e4481de54213040b799809e0777cc8b2fc4efd36678fb2db462827023e8b7016fe3ea96f9c1a9d7
5f93fd9e4ff3f12a37ab2cd383b4c383e502aed0d2625d9a969fd0aaa74fe805eca730606e55ab7ff90c909706ed03
4a2832750c81525e44e0e507f17d36b123467ad9a22ee00c92b395e9dcacbb46c9565bbcd4e7b23756d0bfb70dfea8
8bd43401b7f82caae86ca7123c87594c1f2c50db2808ac39be52c316763976d23048cbbce514e5472716dd9dafdf64
d95d0354e48352febee1dd269ac4a9c0699e3a0e29ef305a91b06a5ade2a2e031ce7f79ce9bf2447e977184eec37cf
a46e9fc7e92bc64905dbfc9bca0efbdcd4804e304139e45b668d46ac8f0873b7dd1c8a45632c6170253dccb4499568
34a63cc7248c685fea6bc215bdd011ea8c56299ceca7304bece925c2112e0e3c54b6997c3c3c5af9d4f9119187e449
ec2b6939d6c27c37585a9f88e06308a783a5f6c5e5ac5b853fab8390531d48be56f3d3dccacf227472fa9d018a328b
07dcbc67447c0cb5f4ed9a1602324e4b9e5759d67c85d3d60a80b93bda1d4d1714504be2faea964093100a6642891c
21b14f6f3b9d53dadf9a69684b2fd43e7b9f0cfe96ccd077cb53f79af237f955a7ff6d786dd7c060662d9dbedfaf75
dc18d3d91507e8d0933266bcb7b6fe171696b290d97efe1260e52edee269decd9f6d3ceb56b694329d4236d50d76d7
655176729f6376d83f2ece6b30781c4d4d8e4491b88f37070898b8a91554b1af6de339d611bb602d2eb84fae2a49cc
6a81c34bf204731702f10821bfe94a856d482a2241df5a3973c39ef6ac0fd624607451504f891c65b51cc7282d9b85
cf392932acbced2a207564d430ab178eeb4d9f83c79e08cc686c5bf0517396b395cb21a0d680040530d95fe14be0e8
32c2cba658b9a9f891070fd6ae105b663485527d4020bd7609e789b2cf6967d64d7b668f5a377be6f4e49f151113d9
93f3e8e1d6fdc38d3b3cfde0505814fdf81744cb40043df293660678407c4b8ffbf754baf717df45bb6763f7becb27
54a23a75cc26564b872a4fad39f08c5b8f6af35ef079acbe3832b323201edfcbbbf6f1e0e424d0ff8cadfc1b397b12
8e3262bf28d2f8fe60da9d7de0be6c1a89ef87626b97943f6811e02888b26a4631118df36d87097d2d51a15e4c4a0d
8ffcc258a0923515f9bf000a9471104ad5d6102e14c88a54338ce6f9fd367cff7cdada98c7ef12d60bdd5e817e9df2
d16aa725f55da2dc85050e6e728982ab9b1de8dab5f05953504cf36066ca2812f0fb1e7833c2d828fab60df804aada
eeadc8db41f95d0ac315bca1a3b1ce958e798dbe54bcbb12987748020a053a1ee24a7922e2262b910acf5425a5bdb6
f62af84d1e8b4279816c7717cb6b8df2db5493b9806834fe41baef9ccf88e8bccc10c8c652814ee88f1f1a7b6464ac
6cc9c43ee9f78dd4f70db59933490c306921d520fd068f122f4f6b11feee607bdb06997c3b4d101e52f8c050a48748
6b30fa401e2c903ddbda1e3dad78200588f24f9f72c4fac79210f2fdba37e7604ca91c6891f8d9d4a762ad51d2e1c2
f2d125edcb4e84dd3094b79fed149fb46e8fa44fe0e3e3047b934e18cddead84f2a2e8040928f673d40459120b86bb
6fbda78e8055977598258 34c2365103b0bfe0bdbec62452249d9b76d79be8c48e96323cf22e2a3e8f21863011e0a10
4ac776e3a2d063e2cd2422896bc6b5f0c6cdaa945105905d98f9ef594a0af1e4d0e8d913de665035072baafad1b6b4
3f38408049cc1c0e849cb7877a0beff0f88efb13f14d544bdd9d50db58c28931cf7f17df6a7c14d83cbf402ff0b1f3
d4b2a093ab0568962c2946a0f8f0f75315dcae5fc57ff51176a9372adf596de3a3d3a37952abe3685e59a70b4c5302
09d35760cbb0553f0db6d051a6427079ef9d69ed2faa89ad1d041ad7f832a9cd3527de6901b0136248c018a61f9c89
92e9ce1f10fd950fa100ae8ed643398cdc8cc4bc517d756303e519eec0c281d871020b1bd22a4734ddf402ff132ed0
48358aa904fd0c93d9a2693d3c9fee907ecd2cb60ba818b790d596773c79aea2d4494f4b075a4bdbb33151c4d07aab
7eae8fc76dee65770155870d8925c282e51a0322e639fe98b172bb8471f1feea152d5941dd20cc13818323c6e9d0f8
ac5bf2d356200bbe392db2b9b4d36d4fa82bb9f261ea10ff61d2333eb39f36bdcc3da2b49d8badead8ebcae9d0688d
ac0e45667fb7e3164dceebd3ecbfefae9b7a42eb92dc951c991f6d414ce247833843fd23830ef662879c22c60a6168
939ce5243c6d9fbd4cfc75d7a70249e21ac224850e4f664ed2094844613562132a20b7e10c93442e1875cadb2a4b2d
f64533b3d6a6c8a20d538a5a503b0c5b18f5156b3c1c5d35ce16d1eb77a3bbe20a461d09215aeac8718c4b726e2b0f
c8236bdee22e6d89da4783e5b1db802af2ca307c068b4665303fa23d558a131ef4fea4ebd4305023a8f8c810495620

aba2174b711b7dd3816d639b8d1b72b5a638e985d8f7ee0e44493a0651deb3c5e7e5b1be3bbc34c49e0e2b228012ce
a2c91c8592daff44feab04c39fa4e2f3f741baf215fc67039519650813c7bc279801dd76e93d86d7e655a2da4c7eec
261744375b6148b7ea5df7f2d1e4b3e697719f076fb87e0fc6c6c4e6dab5e512051dca6beea00833181dd4988a3c47
8610714d3cab01c833acb283ec2bd5e0fc10e5c515c75a84ed57a8b143084bd068b4c5d09abd760b4935ba50075bc2
6ca44e3732971e77436e51469789bf4456e34ac4ad438cb5f0b6ff0e32cba0438fdb39640c302a73fa5e68e5c88f1a
1b746240c0649a0e0d8303a6666f3092d86f7401cc16edda481a1bc4a2d1affd359ae4a532ceb91300000000000003
d8

Wynik użycia powyższego ciągu bajtów oraz klucza JWE_MAC_KEY 852cde285e375dac45ff7c44ee6d12e3
w funkcji haszującej HS256 zwraca 32 bajtową wartość w postaci szesnastkowej:

72ddf916904588e75643b6b0f09938e4cef03e71f0cac0a8e9cd1ac9dd9db985

wydzielając pierwsze 16 bajtów otrzymanego wyniku:

72ddf916904588e75643b6b0f09938e4

po przekodowaniu do formatu Base64URL:

ct35FpBFiOdWQ7aw8Jk45A

otrzymujemy wyliczoną etykietę uwierzytelniającą identyczną z B.3.8a.

B.3.9 Pełna postać obiektu JWE przykładowej komendy przesyłanej do kasy fiskalnej:

eyJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiUlNBMV81Iiwia2lkIjoiY2M4MmQ0YWU0MGY2OGFhMzQyYzQyZDU5YW
M2ZWQ0MDQsQ049TUYgZS1LYXN5In0.hsileeNCtbhjLR60diiBZ7U6kFPqzU3Pc6DDneWQncob1sZTEv7bsqlAv-
QDmR3liTRWuOzcYgduuDwAbmz1xwFI3cVObVeQBiRAgBtFuX_xEpmBdXAzXrMXY37dX1SoCu0Rno0HnBs5bDsnuX4TiZe4
jEKNggOhpf88mErGW26BwU1WbvFlyj9HhEfI2H46D-y29djnkXI_7MpM994hTRTq6JGPE-
9m2ZjOtU6Yw4Ty1kRmUeK9iWQkdIKJHy6TGHD9qnh03Odcyu_DPHJnbmhhB5AaT5yAD9kGcitcMC4PUDju3_qcHgiwPo94
s4m8j1RBo7M8jldVJvvOpU28ng.lkE2bOFzIkxFKpFObeCIww.PoikvBdxUJgfLYAr9tyYOediKO7oQTdEUAPcW6QSKcmP
Cu1e3TKtk-ypKVXtMrJvJd0uRweKpGvx_uyU-IEENg_Dh4o1Q8A7PQ5D2of_qZCW9pXi-
DCnSE6wtPAqgUCYKbeXWdJj8S-jzDrx6z-
nu9ie25f4pw5EnRsA7pGLfk0MIao6oaEDcrmVm646tf9ezCKwACZX3HyOLpN0Q6PtovXPriGV07V7bQ-
MCSsj0AoxKMdjv1YNUGblU-WxAPaSki-
7L54YgkMR3ob9eRUZNAHIzs2jNTAPCuOML2zycO4Qz0saa5h4Q8zuG9WOOaAKJI0CQqHWh3FRqMSOINoXkbay5QVzrZ-
Kbbyf6LusspxI5aibMNPBucrXkodWWszFc3th_jPQ4r6YZB-
RzAO_inRNQqFsTJneP0OJjkd_0SfkanIcU5sjxsbBH9G6Vry5ECtOr5Me3IPcPIXGcdGqBO3TaklpXCHj1-
qOVWeDbZY5xxcQfhhSvYfOtM5ei4yIkNrXIcWTagie-
kmlBnF2mtjm0iv1YCuca8a44RcD5BdpaGOr1lEeizjAPBYi8QWtXSU5KDNXeC0gN4zUNPuccuzPzPk1QaQ7Mt8h9rgzOB9
cDIoOVLFe_hqAq4fn4xG25QKiTVLcOd8PKB8oA4S_f_4nO6cO7zPx_DP4Tu9cBE4M7DJxjZY2d4A21w-
HGx4YukTwaX_w9bcfhKSYNkFYKky6aal80Z4JaMW902NHhleG0ER6c3Y7JFVCyWw9CXIJKfT6BVY8q5CdVFrW4_CF38-
AIuXKRU-
HizqOjM8TrOErY0hOu5443u7KQedT4pyZWyAzVai4MK1Kj5jLUyLOZ4inHPgqTdT3AaTFX5FDwOM_ivUjbwoptwk7MC8eu
oHTXQj02yB4p-
TpdGsx4qO9BHUg3fgFPNbrSFDWn80KNV8C6VmOBaTNZ8MTLkSB3lQhMEC3mYCeB3fMiy_E79NmePsttGKCcCPotwFv4-
qW-cGp11-T_Z5P8_EqN6ss04O0w4PlAq7Q0mJdmpaf0KqnT-
gF7KcwYG5Vq3_5DJCXBu0DSigydQyBUl5E4OUH8X02sSNGetmiLuAMkrOV6dysu0bJVlu81OeyN1bQv7cN_qiL1DQBt_gs
quhspxI8h1lMHyxQ2ygIrDm-UsMWdjl20jBIy7zlFOVHJxbdna_fZNldA1Tkg1L-
vuHdJprEqcBpnjoOKe8wWpGwalreKi4DHOf3nOm_JEfpdxhO7DfPpG6fx-
krxkkF2_ybyg773NSATjBBOeRbZo1GrI8Ic7fdHIpFYyxhcCU9zLRJlWg0pjzHJIxoX-
prwhW90BHqjFYpnOynMEvs6SXCES4OPFS2mXw8PFr51PkRkYfkSewraTnWwnw3WFqfiOBjCKeDpfbF5axbhT-rg5BTHUi-
VvPT3MrPInRy-p0BijKLB9y8Z0R8DLX07ZoWAjJOS55XWdZ8hdPWCoC5O9odTRcUUEvi-
uqWQJMQCmZCiRwhsU9vO51T2t-aaWhLL9Q-e58M_pbM0HfLU_ea8jf5Vaf_bXht18BgZi2dvt-vddwY09kVB-
jQkzJmvLe2_hcWlrKQ2X7-
EmDlLt7iad7Nn20861a2lDKdQjbVDXbXZVF2cp9jdtg_Ls5rMHgcTU2ORJG4jzcHCJi4qRVUsa9t4znWEbtgLS64T64qSc
xqgcNL8gRzFwLxCCG_6UqFbUgqIkHfWjlzw572rA_WJGB0UVBPiRxltRzHKC2bhc85KTKsvO0qIHVk1DCrF47rTZ-
Dx54IzGhsW_BRc5azlcshoNaABAUw2V_hS-
DoMsLLpli5qfiRBw_WrhBbZjSFUn1AIL12CeeJss9pZ9ZNe2aPWjd75vTknxURE9mT8-jh1v3DjTs8_eBQWBT9-
BdEy0AEPfKTZgZ4QHxLj_v3VLr3F99Fu2dj977LJ1SiOnXMJlZLhypPrTnwjFuPavNe8HmsvjgysyMgHt_Lu_bx4OQk0P-
MrfwbOXsSjjJivyjS-
P5g2p194L5sGonvh2Jrl5Q_aBHgKIiyakYxEY3zbYcJfS1RoV5MSg2P_MJYoJI1Ffm_AAqUcRBK1dYQLhTIilQzjOb5_TZ
8_3za2pjH7xLWC91egX6d8tFqpyX1XaLchQUObnKJgqubHejatfBZU1BM82BmyigS8PseeDPC2Cj6tg34BKra7q3I20H5X
QrDFbyho7HOlY55jb5UvLsSmHdIAgoFOh7iSnki4iYrkQrPVCWlvbb2KvhNHotCeYFsdxfLa43y21STuYBoNP5Buu-
cz4jovMwQyMZSgU7ojx8ae2RkrGzJxD7p943U9w21mTNJDDBpIdUg_QaPEi9PaxH-7mB72waZfDtNEB5S-
MBQpIdIazD6QB4skD3b2h49rXggBYjyT59yxPrHkhDy_bo352BMqRxokfjZ1KdirVHS4cLy0SXty06E3TCUt5_tFJ-0bo-
kT-Dj4wR7k04Yzd6thPKi6AQJKPZz1ARZEguGu2-9p46AVZd1mCWDTCNlEDsL_gvb7GJFIknZt215voxI6WMjzyLio-
jyGGMBHgoQSsd246LQY-LNJCKJa8a18MbNqpRRBZBdmPnvWUoK8eTQ6NkT3mZQNQcrqvrRtrQ_OECAScwcDoSct4d6C-
_w-
I77E_FNVEvdnVDbWMKJMc9_F99qfBTYPL9AL_Cx89SyoJOrBWiWLClGoPjw91MV3K5fxX_1EXapNyrfWW3jo9OjeVKr42h

eWacLTFMCCdNXYMuwVT8NttBRpkJwee-
dae0vqomtHQQa1_gyqc01J95pAbATYkjAGKYfnImS6c4fEP2VD6EAro7WQzmM3IzEvFF9dWMD5RnuwMKB2HECCxvSKkc03
fQC_xMu0Eg1iqkE_QyT2aJpPTyf7pB-
zSy2C6gYt5DVlnc8ea6i1ElPSwdaS9uzMVHE0Hqrfq6Px23uZXcBVYcNiSXCguUaAyLmOf6YsXK7hHHx_uoVLVlB3SDME4
GDI8bp0PisW_LTViALvjktsrm0021PqCu58mHqEP9h0jM-s582vcw9orSdi63q2OvK6dBojawORWZ_t-MWTc7r0-
y_766bekLrktyVHJkfbUFM4keDOEP9I4MO9mKHnCLGCmFok5zlJDxtn71M_HXXpwJJ4hrCJIUOT2ZO0glIRGE1YhMqILfh
DJNELhh1ytsqSy32RTOz1qbIog1TilpQOwxbGPUVazwcXTXOFtHrd6O74gpGHQkhWurIcYxLcm4rD8gja97iLm2J2keD5b
HbgCryyjB8BotGZTA_oj1VihMe9P6k69QwUCOo-MgQSVYgq6IXS3EbfdOBbWObjRtytaY46YXY9-4OREk6BlHes8Xn5bG-
O7w0xJ4OKyKAEs6iyRyFktr_RP6rBMOfpOLz90G68hX8ZwOVGWUIE8e8J5gB3XbpPYbX5lWi2kx-
7CYXRDdbYUi36l338tHks-aXcZ8Hb7h-D8bGxObateUSBR3Ka-
6gCDMYHdSYijxHhhBxTTyrAcgzrLKD7CvV4PwQ5cUVx1qE7VeosUMIS9BotMXQmr12C0k1ulAHW8JspE43Mpced0NuUUaX
ib9EVuNKxK1DjLXwtv8OMsugQ4_bOWQMMCpz-
l5o5ciPGht0YkDAZJoODYMDpmZvMJLYb3QBzBbt2kgaG8Si0a_9NZrkpTLOuRM.ct35FpBFiOdWQ7aw8Jk45A

B.4 Przykładowe dane procesu podpisywania danych w środowisku testowym

B.4.1 Pełna postać chronionego nagłówka podpisu danych przesyłanych do repozytorium:


```
{"jpkcertificate":"MIICfjCCAeegAwIBAgIQzILUrkD2iqNCxC1ZrG7UBDANBgkqhkiG9w0BAQsFADAUMRIwEAYDVQQ
DEwlNRiBlLUthc3kwHhcNMTcxMTE1MDk0MDAzWhcNMTkxMTE1MDk0MDAyWjAYMRYwFAYDVQQDEw1aVEUxNzAxMDAwOTAxM
IIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwy3Kc3oTipU45lOIX6K3rruFY83vMqYJqwoWzrRVmZn85cNHSwo
a\/f96AW0\/akADbJ3uo7U8oWhTF\/rj8xIds4uimrN1YiPFmbXAMaeRQDbBa\/qvI5SRQtK9Bmse7KyspIFXVfEWP17Ok
DiBEZ\/n+NC6ERzzKkxA3gMRQFGpHUSQ2+EOi7kykPGi1f8Yh\/2czd+FBvyrp8oSjyX951DdCsqG+rIwlz9p8PeoFwUgg
whb2tMl48U3nD9gZGXLuGOMBZ3nJ9U3fHVdi7XCpvn0PqvTSZLNL45yqXETu6bAZWB5Ab4q5EVvI4unrjnJqc3fPD2OLXp
INIssg6uqyTVCZQIDAQABo0kwRzBFBgNVHQEEPjA8gBDGD6f6PWMBTV\/bee5Lrlc9oRYwFDESMBAGA1UEAxMJTUYgZS1L
YXN5ghCzwtV5n24\/mUCWe9d7xth6MA0GCSqGSIb3DQEBCwUAA4GBAKRTZFPJY5ObY4VVGpJLl4Xb2JNtWpNXdwPs3N8I2
rliGc0dxyq8R4C9X125G0GLgXXXTMDtnE1k+xmCk0aU6bj2xpfezLhW6i1+mmHTB\/2+JhsKp5oRRTXg8SpH5G1vwQI9ek
9B\/bYvn72nKrUaTp3PZsmCNqm1D0VayfTRhZiS","alg":"RS256","jpkmetadata":"eyJjb3JyZWxhdGlvbklkIjoi
VEZELlpURTEyMzQ1Njc4OTAuMjAxOC0wMS0wMVQwMTowMDowMC4wMDBaIn0="}
```


B.4.2 Pełna postać chronionego nagłówka podpisu danych przesyłanych do repozytorium zakodowana w Base64URL:


```
eyJqcGtjZXJ0aWZpY2F0ZSI6Ik1JSUNmakNDQWVlZ0F3SUJBZ0lReklMVXJrRDJpcU5DeEMxWnJHN1VCREFOQmdrcWhraU
c5dzBCQVFzRkFEQVVNUkl3RUFZRFZRUURFd2xOUmlCbExVdGhjM2t3SGhjTk1UY3hNVEUxTURrME1EQXpXaGNOTVRreE1U
RTFNRGswTURBeVdqQVlNUll3RkFZRFZRUURFdzFhVkVVeE56QXhNREF3T1RBeE1JSUJakFOQmdrcWhraUc5dzBCQVFFRk
FBT0NBUThBTUlJQkNnS0NBUUVBd3kzS2Mzb1RpcFU0NWxPSVg2SzNycnVGWTgzdk1xWUpxd29XenJSVm1abjg1Y05IU3dv
YVwvZjk2QVcwXC9ha0FEYkozdW83VThvV2hURlwvcmo4eElkczR1aW1yTjFZaVBGbWJYQU1hZVJRRGJCYVwvcXZJNVNSUX
RLOUJtc2U3S3lzcElGWFZmRVdQMTdPa0RpQkVaXC9uK05DNkVSenpLa3hBM2dNUlFGR3BIVVNRMitFT2k3a3lrUEdpMWY4
WWhcLzJjemQrRkJ2eXJwOG9TanlYOTUxRGRDc3FHK3JJd2x6OXA4UGVvRndVZ2d3aGIydE1sNDhVM25EOWdaR1hMdUdPTU
JaM25KOVUzZkhWZGk3WENwdm4wUHF2VFNaTE5MNDV5cVhFVHU2YkFaV0I1QWI0cTVFVnZJNHVucmpuSnFjM2ZQRDJPTFhw
SU5Jc3NnNnVxeVRWQ1pRSURBUUFCbzBrd1J6QkZCZ05WSFFFRVBqQThnQkRHRDZmNlBXTUJUVlwvYmVlNUxybGM5b1JZd0
ZERVNNQkFHQTFVRUF4TUpUVVlnWlMxTFlYTjVnaEN6d3RWNW4yNFwvbVVDV2U5ZDd4dGg2TUEwR0NTcUdTSWIzRFFFQkN3
VUFBNEdCQUtSVFpGUEpZNU9iWTRWVkdwSkxsNFhiMkpOdFdwTlhkd1BzM044STJybGlHYzBkeHlxOFI0QzlYMTI1RzBHTG
dYWFhUTUR0bkUxayt4bUNrMGFVNmJqMnhwZmV6TGhXNmkxK21tSFRCXC8yK0poc0twNW9SUlRYZzhTcEg1RzF2d1FJOWVr
OUJcL2JZdm43Mm5LclVhVHAzUFpzbUNOcW0xRDBWYXlmVFJoWmlTIiwiYWxnIjoiUlMyNTYiLCJqcGttZXRhZGF0YSI6Im
V5SmpiM0p5Wld4aGRHbHZia2xrSWpvaVZFWkVMbHBVUlRFeU16UTFOamM0T1RBdU1qQXhPQzB3TVMwd01WUXdNVG93TURv
d01DNHdNREJhSW4wPSJ9
```


B.4.3 Przykładowa postać nieskompresowanych danych przesyłanych do repozytorium:


```
{
    "JPK": {
        "naglowek": {
            "wersja": "JPK_KASA_v0-92",
            "dataJPK": "2018-03-30T17:25:26.027Z"
        },
        "podmiot1": {
            "nazwaPod": "Zażółć gęślą jaźń",
            "nrFabr": "ZTE-FAB-0123456789",
            "NIP": "1111111111",
            "adresPod": {
                "ulica": "Ulica",
                "miejsc": "Miejscowość",
                "nrLok": "NrLok",
                "poczta": "Poczta",
                "nrDomu": "NrDomu",
                "kodPoczt": "00-000"
            },
            "nrUnik": "ZTE1234567890",
            "nrEwid": "2018/123456789"
        },
        "content": [
            {
                "zdarzenie": {
                    "pamiecChr": 1,
                    "JPKID": 19,
                    "dataCzas": "2018-03-30T17:25:16.017Z",
                    "typ": {
                        "01": {
```

```
                            "info": "Awaryjne zerowanie pamięci operacyjnej"
                        }
                    }
                }
            }
        ]
    }
}
```


B.4.4 Przykładowa postać danych przesyłanych do repozytorium zakodowana w Base64URL:


```
eyJKUEsiOnsibmFnbG93ZWsiOnsid2Vyc2phIjoiSlBLX0tBU0FfdjAtOTIiLCJkYXRhSlBLIjoiMjAxOC0wMy0zMFQxNz
oyNToyNi4wMjdaIn0sInBvZG1pb3QxIjp7Im5hendhUG9kIjoiWmHFvMOzxYLEhyBnxJnFm2zEhSBqYcW6xYQiLCJuckZh
YnIiOiJaVEUtRkFCLTAxMjM0NTY3ODkiLCJOSVAiOiIxMTExMTExMTExIiwiYWRyZXNQb2QiOnsidWxpY2EiOiJVbGljYS
IsIm1pZWpzYyI6Ik1pZWpzY293b8WbxIciLCJuckxvayI6Ik5yTG9rIiwicG9jenRhIjoiUG9jenRhIiwibnJEb211Ijoi
TnJEb211Iiwia29kUG9jenQiOiIwMC0wMDAifSwibnJVbmlrIjoiWlRFMTIzNDU2Nzg5MCIsIm5yRXdpZCI6IjIwMTgvMT
IzNDU2Nzg5In0sImNvbnRlbnQiOlt7InpkYXJ6ZW5pZSI6eyJwYW1pZWNDaHIiOjEsIkpQS0lEIjoxOSwiZGF0YUN6YXMi
OiIyMDE4LTAzLTMwVDE3OjI1OjE2LjAxN1oiLCJ0eXAiOnsiMDEiOnsiaW5mbyI6IkF3YXJ5am5lIHplcm93YW5pZSBwYW
1pxJljaSBvcGVyYWN5am5laiJ9fX19XX19
```


B.4.5 Pełna postać obiektu JWS przykładowych danych przesyłanych do repozytorium:


```
eyJqcGtjZXJ0aWZpY2F0ZSI6Ik1JSUNmakNDQWVlZ0F3SUJBZ0lRekIMVXJrRDJpcU5DeEMxWnJHN1VCREFOQmdrcWhraUc5dzBCQVFzRkFEQV
VNUkl3RUFZRFZRUURFd2xOUmlCbExVdGhjM2t3SGhjTk1UY3hNVEUxTURrME1EQXpXaGNOTVRreE1URTFNRGswTURBeVdqQVlNUll3RkFZRF
ZRUURFdzFhVkVVeE56QXhNREF3T1RBeE1JSUJakFOQmdrcWhraUc5dzBCQVFFRkFBT0NBUThBTUlJQkNnS0NBUUVBd3kzS2Mzb1RpcFU0N
WxPSVg2SzNycnVGWTgzdk1xWUpxd29XenJSVm1abjg1Y05IU3dvYVwvZjk2QVcwXC9ha0FEYkozdW83VThvV2hURlwvcmo4eElkczR1aW1yTjF
ZaVBGbWJYQU1hZVJRRGJCYVwvcXZJNVNSUXRLOUJtc2U3S3lzcElGWFZmRVdQMTdPa0RpQkVaXC9uK05DNkVSenpLa3hBM2dNUlFGR3BIVV
NRMitFT2k3a3lrUEdpMWY4WWhcLzJjemQrRkJ2eXJwOG9TanlYOTUxRGRDc3FHK3JJd2x6OXA4UGVvRndVZ2d3aGlydE1sNDhVM25EOWdaR
1hMdUdPTUJaM25KOVUzZkhWZGk3WENwdm4wUHF2VFNaTE5MNDV5cVhFVHU2YkFaV0I1QWI0cTVFVnZJNHVucmpuSnFjM2ZQRDJPTFhw
SU5Jc3NnNnVxeVRWQ1pRSURBUUFCbzBrd1J6QkZCZ05WSFFFRVBqQThnQkRHRDZmNlBXTUJUVlwvYmVlNUxybGM5b1JZd0ZERVNNQkFHQ
TFVRUF4TUpUVVlnWlMxTFlYTjVnaEN6d3RWNW4yNFwvbVVDV2U5ZDd4dGg2TUEwR0NTcUdTSWIzRFFFQkN3VUFBNEdCQUtSVFpGUEpZN
U9iWTRWVkdwSkxsNFhiMkpOdFdwTlhkd1BzM044STJybGlHYzBkeHlxOFI0QzlYMTI1RzBHTGdYWFhUTUR0bkUxayt4bUNrMGFVNmJqMnhw
ZmV6TGhXNmkxK21tSFRCXC8yK0poc0twNW9SUlRYZzhTcEg1RzF2d1FJOWVrOUJcL2JZdm43Mm5LclVhVHAzUFpzbUNOcW0xRDBWYXlmVFJ
oWmlTliwiYWxnIjoiUlMyNTYiLCJqcGttZXRhZGF0YSI6ImV5SmpiM0p5Wld4aGRHbHZia2xrSWpvaVZFWkVMbHBVUlRFeU16UTFOamM0T1RB
dU1qQXhPQzB3TVMwd01WUXdNVG93TURvd01DNHdNREJhSW4wPSJ9.eyJKUEsiOnsibmFnbG93ZWsiOnsid2Vyc2phIjoiSlBLX0tBU0FfdjAtOT
IiLCJkYXRhSlBLIjoiMjAxOC0wMy0zMFQxNzoyNToyNi4wMjdaIn0sInBvZG1pb3QxIjp7Im5hendhUG9kIjoiWmHFvMOzxYLEhyBnxJnFm2zEhSBq
YcW6xYQiLCJuckZhYnIiOiJaVEUtRkFCLTAxMjM0NTY3ODkiLCJOSVAiOiIxMTExMTExMTExIiwiYWRyZXNQb2QiOnsidWxpY2EiOiJVbGljYSIsIm1p
ZWpzYyI6Ik1pZWpzY293b8WbxIciLCJuckxvayI6Ik5yTG9rIiwicG9jenRhIjoiUG9jenRhIiwibnJEb211IjoiTnJEb211Iiwia29kUG9jenQiOiIwMC0wM
DAifSwibnJVbmlrIjoiWlRFMTIzNDU2Nzg5MCIsIm5yRXdpZCI6IjIwMTgvMTIzNDU2Nzg5In0sImNvbnRlbnQiOlt7InpkYXJ6ZW5pZSI6eyJwYW1pZ
WNDaHIiOjEsIkpQS0lEIjoxOSwiZGF0YUN6YXMiOiIyMDE4LTAzLTMwVDE3OjI1OjE2LjAxN1oiLCJ0eXAiOnsiMDEiOnsiaW5mbyI6IkF3YXJ5am5lI
Hplcm93YW5pZSBwYW1pxJljaSBvcGVyYWN5am5laiJ9fX19XX19.upliPTXaTwHTJrtHMFJ5reFugWpY595RLwIruU9mto3XitQzTvgQqCL-VUm0-
XobYzpjk7r3p45H2Dux0KuxEzwZqpE9RdU2bnY6QOCiBrmwdZGwEhXln6Hxr-rTOy2Wn24fVOry3MtqzMhtdjA9fdfyXTbbooh9Yp1ckN-
YX2uoSlqB6BbkVfwopDLoPdSZFvGMaub4mWox3dSlgf7DXaajvemFvHARtkzzj0hlg28M2pJleJP77x6d5b3RPNw-ZqGFwaJZZtXqf_hnE4e1bIx-
pwXIC2C1hgCY7vDXLCXYM9nePCevL8yZ0Wc1rjVsiCiqzoEyzyMyMS2VTIUZeQ
```

B.5 Przykładowe dane procesu szyfrowania danych w środowisku testowym

B.5.1 Pełna postać chronionego nagłówka obiektu JWE danych przesyłanych z kasy:

{"kid":"3A00000008E68F55815D4EA63A000100000008, CN=eKasy-SubCA","enc":"A128CBC-HS256","alg":"RSA1_5"}

B.5.2 Pełna postać chronionego nagłówka obiektu JWE danych przesyłanych z kasy fiskalnej zakodowana w Base64URL:

eyJraWQiOiIzQTAwMDAwMDA4RTY4RjU1ODE1RDRFQTYzQTAwMDEwMDAwMDAwOCwgQ049ZUthc3ktU3ViQ0EiLCJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiUlNBMV81In0

B.5.3 Wartości przykładowych danych użytych do szyfrowania:

JWE_AES_CEK => 0fae0202c8aa5d39bac1b9f58a9f440c4b700abdffd7e661ac4c609e288529be

JWE_MAC_KEY => 0fae0202c8aa5d39bac1b9f58a9f440c
JWE_AES_KEY => 4b700abdffd7e661ac4c609e288529be

JWE_AES_IV => c773654a97535031619a525f4285f3dd

B.5.4 Zaszyfrowana wartość przykładowego klucza algorytmu szyfrującego algorytmem asymetrycznym RSA z wykorzystaniem klucza publicznego ministerstwa zakodowana w Base64URL:

giC4C064EjKUdWmh0TmoQVuXbxByz5yWO53Hxda3Je1gRchNmnq0s38RXyJt9L1e3SDe5hnZuVtgPKufUBgEblItprryumGYnqyhuzIbD0m8akTq9JyJHQ7SERZlGYIzAgQbIn7NJAKswtzhpP56PxSnMRwegdx0PoW-ZlTx2dYSpHRobWYvpHjz4t25H_poYZh2nAmmzC4nWOGnlshNI0qxk21E64_Tb-4ACpoqvk6WlPGygUYT4M1hoAN4w_P0fsTyQxcmsXt3RpfiCbCROY2oLyQYGVYnTodbpLp7T4kVKN3XnzT6szBFzMCJsQ9B0Ug26mQARkH0cx7FWOtVCg

B.5.5 Przykładowa wartość wektora inicjującego zakodowana w Base64URL:

x3NlSpdTUDFhmlJfQoXz3Q

B.5.6 Przykładowa wartość zaszyfrowanych danych zakodowana w Base64URL:

jnYxL4MrKbWmgY5ZeUrL_etV-byYTeEwp8fH1j5q8ii54kYWQPUBErh3APg7KLl8ZjY644HdbcZgy168x0cACpVhh5MqA93K5CXl0e-4VUH97iBcHo_VdzUW_iqX3HPyfl1WLrt2PgIiqFOuzjapVYiVFzmXwhKsoWx4oYzIJfUJYM1QFcHnPVWPONlTnpDV6VRsskm3oC4sCn9DW0TJ-h8HHzvXT18n6F1SHLrqcVgfb4cpz5w6X_k8TBPXaJNgOvEgcbUTXNkKkUWs2xTKNdJAinKTzXR9WFsPajd6R5brwVIEpRgsHy6icr4RyxGO7fPS8JmKsbEY2CqedVO62ZtYREH1K2giji5lXPEpLPa7kFHdJ4uknjOjbgK-_Kbb9BUVdhdFO6-bNpT67fiReZ--JLyu-cAYVnoTMj0GqSXOjNLiPZbVG1Q3Q02yw875kPf0nrlPihkNoCGgdBgP66mvF0CdP-0hoZiMYKh9qOzeAtuiDb0kQL91mPexz_YZ1GQs-UrkYP85Fnv-vpvPkgBp9kJl9x1SiB4qvj86Ryaf-ic8P_FvOy9bPv9wRtGIaDTcJBuK0vaIb7W7FCYiBKyKv6oR0vsoXghHS8NrH7ARm0VIC-q9v_S8exfy5Rik6znN51Qwsdz5qG0b-rQU5Gs1hLFckc8Ra1wDMvyfv6qSE6-dbpmbIsw9rCh2tvNzwM2nN4cHMZQErfpa8-bTuGcRehZVwrjmfYkV9kcWqbSVajJfWAzeZLmjmcU3hytB6Ke7Yo2HyIjtQNqfWyWY4JmpgqSEVexk6MxeBQr35s2LKZ8HouO7jqqPV1RHh_oFIxNcaleisxh4nuEm3T8OfXU8UHvdjRHu2V_HjLZFFtuzT51iydzcHCUVK020mNqF92mMg3w3p6VTe6xBtteuwIfG5uORdfw9Onu1u3e-PVe7P3H27iuPvLdS-hG0ywN8aissvnDrIe2gKL_Na7Cuf_9XGv2EHXEEFqYJ67GUiDMYEK1M3JVM0QiQ0zFL1llPwyN9nHdXRyfneWo4931krUeUYh-yxAtmgeH2lkT67pQ6jwZrqXS9WVBpBdN5JzMS8RjJShZY2BEotJp5MqMdz-IfZwnx07JBjuMobskg_1yPmtCWQXoAb-MA574jiV40EEKq9HkS27T59wOS-XdOi32KJHs3a9b1pSgmZqiWSUpwLaOuuZYjV9H7_sz5i6w8oCByxrcOLcjY1T2cp0HIaHiM1LnHrDvmAN0Weh1rthK2I4Esy9yHfl1RjFwzoUmSz5sYdnx2jqKOEskAiaqc45IMTEdFIV8pWJcFsaxMx1CjUeumu_IGom0aiMDikvAyrs-BmFwIOVSRzIsyezngh HS6K5H3R9isuiTA64OkomnqKIcC2TFjmx97EAjMGG3CBqc7fzdPMDcCYRoTgrq8JF-gjYED4RBAZ8cZYBJx77neOpZ-Kdy_8h3zT70GmJzmzjshrqDnPV3CdT_T7JCPWPoE0cQk2oUIvKCnx3DsH6x_1tti6FkzfdqAcGj7VftQN5XAwVcmMBZQwhChFS945C1soRD1SLWqWfaxG0CBqu5rVfwODOZsV4WAxX0XjrE6CbDbeLuCrzcjTto3rcRnrsVAWb-fnC97FEsevL4Lfg7S7iE8YRCR1QW3M4OaI-46SHMBov2u92RdPvzLpYjIf3N29YmijYkFMcYnfVlt7-

```
U2Ou9YpNNhF5h2veEHzWUS07gyy-pSOtkjLXwp2MpKQucf3jyXJWyuArU4qVAaN-E-
WZkO1oNI_5zFb3W26AbEoumrhL8FpY8P5KGYAgH1B3uVNs2TQzdb3cAg4lIe9PBeeNtMi2-m505-
r1ljd0uLhmaZeidaCYdr4V50AiC3y4ggd6R4GE0u6QXttdCgwvRWAHUUBtzT4RONe4-KzcZVGK3Is2zGQL-
HrTii_oOgmDBpdTsnWTX8wFBITUw_tKf7YOZbwedLk8QVLYKji9ZdlPOek-w-
zRXaYDTQotleP4oRdMy4wmPn1mHsdF8RJ0UCQ8YrRF1Fz7ogp9C8ftU3YpGo9QxfKyaw46TsiGlQrEBCQ3r8gRNOTXHcCs
O4l-3iB05u4pDhZzz-7WbHltXGuDqFik7BWnq-
V0wRhX7KXei3ikGSsp5eCrigbHWsci_QdCmj5YjR5FV7Av29VqkZScCKZQ4_f4SHiYPuM7hurB56qLmpBlhkvxUZHyvp0u
PCa-vDgSn0FQ23dAVvmUI6epkad_-YwUtOthCJvfphZeiH8rvAOr1p1YM71EEkW-
u5xrCrdHtBy7NQpGCVYs_Cm6g_UIfguOrgOBmvgEKQlKapuLLi_rGwHsSNOlnMA9yx3sC4PGTeIAHca1wtOp1sFQwUxcgE
QRV8TY86G17qlrQIs-v9-
uDwSEI7aZpqGfZmZKaQOWCno23i4XbDQnnnjCdF1fmMxACorg5g_Wjcpgs91fPiePv9_1YYEnXRPduqhQbVb1J2txdOoSM
CrG9RZesYhV0KBvLOHBbhFBCD-
5IApXXIJ3It2aU2HJUtD77B60U2dOlZ6RzQ2OvmNgJ8oUSozKplTiYaDLKE3mgMO4o2IksZjvKISi69MmSJy059vQXkPBG
AJ3hDlHsCwrxCg43ZvbcV2T55466HhsBv8WAtTl01psYO0IBAp2QgbFfkZkYEaP5XgLmdtAGBJwPjSSgH4dM31MgbgRXyd
yo9qoEFUJj3-bzYMGoP5mSidKQguzYv7_fuClBzAeq_iYHdqLaXK-tSq0_mHw2jLgVPGYk-
02UZwUEUINqqXnfd04YPQ04XgmtrieqJzTaQH3xGpD2N2u-Z8VqaJkYD-
k99_Qftu0WUYOWvWaw0vgTATN_Vu2EgPB9uOSC5Ul7jmiieGAf5O7yTlivMdU2hMETPrsa-
FXomu56nzu0kxE0rx7h_Ckf2fDI3QatBSSnyndmK3jWiEttE65U_8-wJSU8Js_mE5-
MtXDBk9qobRfMcJpfzAgatdD7RWRyuIV85rERPOqKfaoqe_xt1iuW8zNhy634zLx6kv_aKI6d8jE1QgO0qZIdgRcKqpP1z
SPmC2rf1Z7ReOCtH_pc97Nj_0pXQBzftI3oWhnF6gpTtROKHn6-kbvne249vASSPM70UO9y8PXyMK-
kQGT8GGsmreAlWh1SFOMgiN-cfRrlGxHTAn0w
```

B.5.7a Przykładowa wartość dodatkowych danych uwierzytelniających:

```
eyJraWQiOiIzQTAwMDAwMDA4RTY4RjU1ODE1RDRFQTYzQTAwMDEwMDAwMDAwOCwgQ049ZUthc3ktU3ViQ0EiLCJlbmMiOi
JBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiUlNBMV81In0
```

B.5.7b Przykład wyliczenia reprezentacji wartości długości dodatkowych danych uwierzytelniających zakodowana w Base64URL:

```
JWE_AAD_URL BYTES LENGTH -> 135

JWE_AAD_URL BITS LENGTH -> 135 * 8 = 1080

JWE_AT = [0, 0, 0, 0, 0, 0, 4, 56]
```

odzwierciedlenie w postaci szesnastkowej:

```
0000000000000438
```

B.5.8a Przykładowa wartość etykiety uwierzytelniającej zakodowana w Base64URL:

```
-x_YGNfKRdmlmIdWG7qxEA
```

odzwierciedlenie w postaci szesnastkowej:

```
fb1fd818d7ca45d9a59887561bbab110
```

B.5.8b Przykład wyliczenia wartości etykiety uwierzytelniającej przykładowych danych:

Postać szesnastkowa odszyfrowanego 32 bajtowego klucza CEK (Content Encryption Key) B.5.3:

```
0fae0202c8aa5d39bac1b9f58a9f440c4b700abdffd7e661ac4c609e288529be
```

pierwsze 16 bajtów wykorzystywane jako klucz w funkcji HMAC (JWE_MAC_KEY):

postać szesnastkowa wykorzystana w funkcji HMAC:
0fae0202c8aa5d39bac1b9f58a9f440c

użyte dane autoryzujące AAD (nagłówek JWE) B.5.7a:

```
postać ASCII:
{"kid":"3A00000008E68F55815D4EA63A000100000008, CN=eKasy-SubCA","enc":"A128CBC-
HS256","alg":"RSA1_5"}
```

postać Base64URL:
eyJraWQiOiIzQTAwMDAwMDA4RTY4RjU1ODE1RDRFQTYzQTAwMDEwMDAwMDAwOCwgQ049ZUthc3ktU3ViQ0EiLCJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiUlNBMV81In0

postać szesnastkowa (bajty postaci Base64URL) wykorzystana w funkcji HMAC:
65794a72615751694f69497a515441774d4441774d4441345254593452655154597a515441774d4445774d4441774d4441774f437767513034395a55746863336b7455335669513045694c434a6c626d4d694f694a424d54493451304a444c5568544d6a5532496977695957786e496a6f69556c4e424d563831496e30

użyty 16 bajtowy wektor inicjujący IV B.5.5:

postać Base64URL:
x3NlSpdTUDFhmlJfQoXz3Q

postać szesnastkowa wykorzystana w funkcji HMAC:
c773654a97535031619a525f4285f3dd

zaszyfrowane dane użyte do wyliczenia etykiety uwierzytelniającej B.5.6:

postać Base64URL:
jnYxL4MrKbWmgY5ZeUrL_etV-
byYTeEwp8fH1j5q8ii54kYWQPUBErh3APg7KLl8ZjY644HdbcZgy168x0cACpVhh5MqA93K5CXl0e-
4VUH97iBcHo_VdzUW_iqX3HPyfl1WLrt2PgIiqFOuzjapVYiVFzmXwhKsoWx4oYzIJfUJYM1QFcHnPVWPONlTnpDV6VRss
km3oC4sCn9DW0TJ-
h8HHzvXT18n6F1SHLrqcVgfb4cpz5w6X_k8TBPXaJNgOvEgcbUTXNkKkUWs2xTKNdJAinKTzXR9WFsPajd6R5brwVIEpRg
sHy6icr4RyxGO7fPS8JmKsbEY2CqedVO62ZtYREH1K2giji5lXPEpLPa7kFHdJ4uknjOjbgK-_Kbb9BUVdhdFO6-
bNpT67fiReZ--JLyu-cAYVnoTMj0GqSXOjNLiPZbVG1Q3Q02yw875kPf0nrlPihkNoCGgdBgP66mvF0CdP-
0hoZiMYKh9qOzeAtuiDb0kQL91mPexz_YZ1GQs-UrkYP85Fnv-vpvPkgBp9kJl9x1SiB4qvj86Ryaf-
ic8P_FvOy9bPv9wRtGIaDTcJBuK0vaIb7W7FCYiBKyKv6oR0vsoXghHS8NrH7ARm0VIC-
q9v_S8exfy5Rik6znN51Qwsdz5qG0b-rQU5Gs1hLFckc8Ra1wDMvyfv6qSE6-
dbpmbIsw9rCh2tvNzwM2nN4cHMZQErfpa8-
bTuGcRehZVwrjmfYkV9kcWqbSVajJfWAzeZLmjmcU3hytB6Ke7Yo2HyIjtQNqfWyWY4JmpgqSEVexk6MxeBQr35s2LKZ8H
ouO7jqqPV1RHh_oFIxNcaleisxh4nuEm3T8OfXU8UHvdjRHu2V_HjLZFFtuzT51iydzcHCUVK020mNqF92mMg3w3p6VTe6
xBtteuwIfG5uORdfw9Onu1u3e-PVe7P3H27iuPvLdS-
hG0ywN8aissvnDrIe2gKL_Na7Cuf_9XGv2EHXEEFqYJ67GUiDMYEK1M3JVM0QiQ0zFL1llPwyN9nHdXRyfneWo4931krUe
UYh-yxAtmgeH2lkT67pQ6jwZrqXS9WVBpBdN5JzMS8RjJShZY2BEotJp5MqMdz-
IfZwnx07JBjuMobskg_1yPmtCWQXoAb-MA574jiV40EEKq9HkS27T59wOS-
XdOi32KJHs3a9b1pSgmZqiWSUpwLaOuuZYjV9H7_sz5i6w8oCByxrcOLcjY1T2cp0HIaHiM1LnHrDvmAN0Weh1rthK2I4E
sy9yHfl1RjFwzoUmSz5sYdnx2jqKOEskAiaqc45IMTEdFIV8pWJcFsaxMx1CjUeumu_IGom0aiMDikvAyrs-
BmFwIOVSRzIsyeznghHS6K5H3R9isuiTA64OkomnqKIcC2TFjmx97EAjMGG3CBqc7fzdPMDcCYRoTgrq8JF-
gjYED4RBAZ8cZYBJx77neOpZ-
Kdy_8h3zT70GmJzmzjshrqDnPV3CdT_T7JCPWPoE0cQk2oUIvKCnx3DsH6x_1tti6FkzfdqAcGj7VftQN5XAwVcmMBZQwh
ChFS945C1soRD1SLWqWfaxG0CBqu5rVfwODOZsV4WAxX0XjrE6CbDbeLuCrzcjTto3rcRnrsVAWb-
fnC97FEsevL4Lfg7S7iE8YRCR1QW3M4OaI-46SHMBov2u92RdPvzLpYjIf3N29YmijYkFMcYnfVlt7-
U2Ou9YpNNhF5h2veEHzWUS07gyy-pSOtkjLXwp2MpKQucf3jyXJWyuArU4qVAaN-E-
WZkO1oNI_5zFb3W26AbEoumrhL8FpY8P5KGYAgH1B3uVNs2TQzdb3cAg4lIe9PBeeNtMi2-m505-
r1ljd0uLhmaZeidaCYdr4V50AiC3y4ggd6R4GE0u6QXttdCgwvRWAHUUBtzT4RONe4-KzcZVGK3Is2zGQL-
HrTii_oOgmDBpdTsnWTX8wFBITUw_tKf7YOZbwedLk8QVLYKji9ZdlPOek-w-
zRXaYDTQotleP4oRdMy4wmPn1mHsdF8RJ0UCQ8YrRF1Fz7ogp9C8ftU3YpGo9QxfKyaw46TsiGlQrEBCQ3r8gRNOTXHcCs
O4l-3iB05u4pDhZzz-7WbHltXGuDqFik7BWnq-
V0wRhX7KXei3ikGSsp5eCrigbHWsci_QdCmj5YjR5FV7Av29VqkZScCKZQ4_f4SHiYPuM7hurB56qLmpBlhkvxUZHyvp0u
PCa-vDgSn0FQ23dAVvmUI6epkad_-YwUtOthCJvfphZeiH8rvAOr1p1YM71EEkW-
u5xrCrdHtBy7NQpGCVYs_Cm6g_UIfguOrgOBmvgEKQlKapuLLi_rGwHsSNOlnMA9yx3sC4PGTeIAHca1wtOp1sFQwUxcgE
QRV8TY86G17qlrQIs-v9-
uDwSEI7aZpqGfZmZKaQOWCno23i4XbDQnnnjCdF1fmMxACorg5g_Wjcpgs91fPiePv9_1YYEnXRPduqhQbVb1J2txdOoSM
CrG9RZesYhV0KBvLOHBbhFBCD-
5IApXXIJ3It2aU2HJUtD77B60U2dOlZ6RzQ2OvmNgJ8oUSozKplTiYaDLKE3mgMO4o2IksZjvKISi69MmSJy059vQXkPBG
AJ3hDlHsCwrxCg43ZvbcV2T55466HhsBv8WAtTl01psYO0IBAp2QgbFfkZkYEaP5XgLmdtAGBJwPjSSgH4dM31MgbgRXyd
yo9qoEFUJj3-bzYMGoP5mSidKQguzYv7_fuClBzAeq_iYHdqLaXK-tSq0_mHw2jLgVPGYk-
02UZwUEUINqqXnfd04YPQ04Xgmtrieqj zTaQH3xGpD2N2u-Z8VqaJkYD-
k99_Qftu0WUYOWvWaw0vgTATN_Vu2EgPB9uOSC5Ul7jmiieGAf5O7yTlivMdU2hMETPrsa-
FXomu56nzu0kxE0rx7h_Ckf2fDI3QatBSSnyndmK3jWiEttE65U_8-wJSU8Js_mE5-
MtXDBk9qobRfMcJpfzAgatdD7RWRyuIV85rERPOqKfaoqe_xt1iuW8zNhy634zLx6kv_aKI6d8jE1QgO0qZIdgRcKqpP1z
SPmC2rf1Z7ReOCtH_pc97Nj_0pXQBzftI3oWhnF6gpTtROKHn6-kbvne249vASSPM70UO9y8PXyMK-
kQGT8GGsmreAlWh1SFOMgiN-cfRrlGxHTAn0w

postać szesnastkowa wykorzystana w funkcji HMAC:
8e76312f832b29b5a6818e59794acbfdeb55f9bc984de130a7c7c7d63e6af228b9e2461640f50112b87700f83b28b97c66363ae381dd6dc660cb5ebcc747000a956187932a03ddcae425e5d1efb85541fdee205c1e8fd5773516fe2a97dc73f27e5d562ebb763e0222a853aece36a9558895173997c212aca16c78a18cc825f50960cd5015c1e73d558f38d953

9e90d5e9546cb249b7a02e2c0a7f435b44c9fa1f071f3bd74f5f27e85d521cbaea71581f6f8729cf9c3a5ff93c4c13
d76893603af12071b5135cd90a9145acdb14ca35d2408a7293cd747d585b0f6a377a4796ebc15204a5182c1f2ea272
be11cb118eedf3d2f0998ab1b118d82a9e7553bad99b584441f52b68228e2e655cf1292cf6bb9051dd278ba49e33a3
6e02befca6dbf415157617453baf9b3694faedf891799fbe24bcaef9c018567a13323d06a925ce8cd2e23d96d51b54
37434db2c3cef990f7f49eb94f8a190da021a074180feba9af17409d3fed21a1988c60a87da8ecde02dba20dbd2440
bf7598f7b1cff619d4642cf94ae460ff39167bfebe9bcf920069f64265f71d52881e2abe3f3a47269ffa273c3ff16f
3b2f5b3eff7046d1886834dc241b8ad2f6886fb5bb14262204ac8abfaa11d2fb285e08474bc36b1fb0119b45480bea
bdbff4bc7b17f2e518a4eb39cde75430b1dcf9a86d1bfab414e46b3584b15c91cf116b5c0332fc9fbfaa9213af9d6e
999b22cc3dac2876b6f373c0cda7378707319404adfa5af3e6d3b867117a1655c2b8e67d8915f64716a9b4956a325f
580cde64b9a399c537872b41e8a7bb628d87c888ed40da9f5b2598e099a982a48455ec64e8cc5e050af7e6cd8b299f
07a2e3bb8eaa8f57544787fa0523135c6a57a2b318789ee126dd3f0e7d753c507bdd8d11eed95fc78cb64516dbb34f
9d62c9dcdc1c25152b4db498da85f7698c837c37a7a5537bac41b6d7aec087c6e6e39175fc3d3a7bb5bb77be3d57bb
3f71f6ee2b8fbcb752fa11b4cb037c6a2b2cbe70eb21eda028bfcd6bb0ae7fff571afd841d710416a609ebb1948833
1810ad4cdc954cd10890d3314bd6594fc3237d9c77574727e7796a38f77d64ad4794621fb2c40b6681e1f69644faee
943a8f066ba974bd59506905d379273312f118c94a1658d81128b49a7932a31dcfe21f6709f1d3b2418ee3286ec920
ff5c8f9ad096417a006fe300e7be23895e341042aaf47912dbb4f9f70392f9774e8b7d8a247b376bd6f5a5282666a8
96494a702da3aeb9962357d1fbfeccf98bac3ca02072c6b70e2dc8d8d53d9ca741c868788cd4b9c7ac3be600dd167a
1d6bb612b623812ccbdc877e5d518c5c33a14992cf9b18767c768ea28e12c90089aa9ce3920c4c4745215f29589705
b1ac4cc750a351eba6bbf206a26d1a88c0e292f032aecf81985c08395491cc8b327b39e08474ba2b91f747d8acba24
c0eb83a4a269ea288702d931639b1f7b1008cc186dc206a73b7f374f303702611a1382babc245fa08d8103e1104067
c719601271efb9de3a967e29dcbff21df34fbd06989ce6ce3b21aea0e73d5dc2753fd3ec908f58fa04d1c424da8508
bca0a7c770ec1fac7fd6db62e859337dda807068fb55fb503795c0c15726301650c210a1152f78e42d6ca110f548b5
aa59f6b11b4081aaee6b55fc0e0ce66c578580c57d178eb13a09b0db78bb82af37234eda37adc467aec54059bf9f9c
2f7b144b1ebcbe0b7e0ed2ee213c611091d505b733839a23ee3a487301a2fdaef7645d3efccba588c87f7376f589a2
8d890531c6277d596defe5363aef58a4d361179876bde107cd6512d3b832cbea523ad9232d7c29d8ca4a42e71fde3c
97256cae02b538a9501a37e13e59990ed68348ff9cc56f75b6e806c4a2e9ab84bf05a58f0fe4a1980201f5077b9536
cd9343375bddc020e2521ef4f05e78db4c8b6fa6e74e7eaf5963774b8b8666997a275a09876be15e740220b7cb8820
77a478184d2ee905edb5d0a0c2f45600751406dcd3e1138d7b8f8acdc65518adc8b36cc640bf87ad38a2fe83a09830
69753b275935fcc050484d4c3fb4a7fb60e65bc1e74b93c4152d82a38bd65d94f39e93ec3ecd15da6034d0a2d95e3f
8a1174ccb8c263e7d661ec745f1127450243c62b445d45cfba20a7d0bc7ed5376291a8f50c5f2b26b0e3a4ec886950
ac4042437afc81134e4d71dc0ac3b897ede2074e6ee290e1673cfeed66c796d5c6b83a858a4ec15a7abe574c11857e
ca5de8b78a4192b29e5e0ab8a06c75ac722fd07429a3e588d1e4557b02fdbd56a91949c08a650e3f7f84878983ee33
b86eac1e7aa8b9a9065864bf15191f2be9d2e3c26bebc38129f4150db774056f99423a7a991a77ff98c14b4eb61089
bdfa6165e887f2bbc03abd69d5833bd441245bebb9c6b0ab747b41cbb350a4609562cfc29ba83f5087e0b8eae03819
af80429094a6a9b8b2e2feb1b01ec48d3a59cc03dcb1dec0b83c64de2001dc6b5c2d3a9d6c150c14c5c80441157c4d
8f3a1b5eea96b408b3ebfdfae0f048423b699a6a19f66664a6903960a7a36de2e176c34279e78c2745d5f98cc400a8
ae0e60fd68dca60b3dd5f3e278fbfdff56181275d13ddbaa8506d56f5276b7174ea12302ac6f5165eb18855d0a06f2
ce1c16e1141083fb9200a575c827722dd9a5361c952d0fbec1eb453674e959e91cd0d8ebe636027ca144a8ccaa654e
261a0cb284de680c3b8a36224b198ef2884a2ebd326489cb4e7dbd05e43c1180277843947b02c2bc42838dd9bdb715
d93e79e3ae8786c06ff1602d4e5d35a6c60ed08040a764206c57e466460468fe5780b99db401812703e3492807e1d3
37d4c81b8115f2772a3daa81055098f7f9bcd8306a0fe664a274a420bb362feff7ee0a507301eabf8981dda8b6972b
eb52ab4fe61f0da32e054f19893ed36519c1411420daaa5e77ddd3860f434e17826b6b89ea89cd36901f7c46a43d8d
daef99f15a9a264603fa4f7dfd07edbb459460e5af59ac34be04c04cdfd5bb61203c1f6e3920b9525ee39a289e1807
f93bbc93962bcc754da13044cfaec6be157a26bb9ea7ceed24c44d2bc7b87f0a47f67c323741ab414929f29dd98ade
35a212db44eb953ff3ec09494f09b3f984e7e32d5c3064f6aa1b45f31c2697f30206ad743ed1591cae215f39ac444f
3aa29f6a8a9eff1b758ae5bcccd872eb7e332f1ea4bff68a23a77c8c4d5080ed2a64876045c2aaa4fd7348f982dab7
f567b45e382b47fe973decd8ffd295d00737ed237a1686717a8294ed44e2879fafa46ef9dedb8f6f01248f33bd143b
dcbc3d7c8c2be910193f061ac9ab78095687548538c82237e71f46b946c474c09f4c

długość dodatkowych danych autoryzujących w formacie Base64URL wynosi 123 bajty, czyli 984 bity i w formacie Big-Endian w postaci szesnastkowej ma wartość B.5.7b:

0000000000000438

Dokonując konkatenacji bajtowej AAD, IV oraz danych zaszyfrowanych i długości AAD do wyliczenia MAC będzie wykorzystany ciąg bajtów w postaci szesnastkowej:

65794a72615751694f69497a515441774d4441774d4441345254593452655154597a515441
774d4445774d4441774d4441774f437767513034395a55746863336b7455335669513045694c434a6c626d4d694f69
4a424d54493451304a444c5568544d6a5532496977695957786e496a6f69556c4e424d563831496e30c773654a9753
5031619a525f4285f3dd8e76312f832b29b5a6818e59794acbfdeb55f9bc984de130a7c7c7d63e6af228b9e2461640
f50112b87700f83b28b97c66363ae381dd6dc660cb5ebcc747000a956187932a03ddcae425e5d1efb85541fdee205c
1e8fd5773516fe2a97dc73f27e5d562ebb763e0222a853aece36a9558895173997c212aca16c78a18cc825f50960cd
5015c1e73d558f38d9539e90d5e9546cb249b7a02e2c0a7f435b44c9fa1f071f3bd74f5f27e85d521cbaea71581f6f
8729cf9c3a5ff93c4c13d76893603af12071b5135cd90a9145acdb14ca35d2408a7293cd747d585b0f6a377a4796eb
c15204a5182c1f2ea272be11cb118eedf3d2f0998ab1b118d82a9e7553bad99b584441f52b68228e2e655cf1292cf6
bb9051dd278ba49e33a36e02befca6dbf415157617453baf9b3694faedf891799fbe24bcaef9c018567a13323d06a9
25ce8cd2e23d96d51b5437434db2c3cef990f7f49eb94f8a190da021a074180feba9af17409d3fed21a1988c60a87d
a8ecde02dba20dbd2440bf7598f7b1cff619d4642cf94ae460ff39167bfebe9bcf920069f64265f71d52881e2abe3f

3a47269ffa273c3ff16f3b2f5b3eff7046d1886834dc241b8ad2f6886fb5bb14262204ac8abfaa11d2fb285e08474b
c36b1fb0119b45480beabdbff4bc7b17f2e518a4eb39cde75430b1dcf9a86d1bfab414e46b3584b15c91cf116b5c03
32fc9fbfaa9213af9d6e999b22cc3dac2876b6f373c0cda7378707319404adfa5af3e6d3b867117a1655c2b8e67d89
15f64716a9b4956a325f580cde64b9a399c537872b41e8a7bb628d87c888ed40da9f5b2598e099a982a48455ec64e8
cc5e050af7e6cd8b299f07a2e3bb8eaa8f57544787fa0523135c6a57a2b318789ee126dd3f0e7d753c507bdd8d11ee
d95fc78cb64516dbb34f9d62c9dcdc1c25152b4db498da85f7698c837c37a7a5537bac41b6d7aec087c6e6e39175fc
3d3a7bb5bb77be3d57bb3f71f6ee2b8fbcb752fa11b4cb037c6a2b2cbe70eb21eda028bfcd6bb0ae7fff571afd841d
710416a609ebb19488331810ad4cdc954cd10890d3314bd6594fc3237d9c77574727e7796a38f77d64ad4794621fb2
c40b6681e1f69644faee943a8f066ba974bd59506905d379273312f118c94a1658d81128b49a7932a31dcfe21f6709
f1d3b2418ee3286ec920ff5c8f9ad096417a006fe300e7be23895e341042aaf47912dbb4f9f70392f9774e8b7d8a24
7b376bd6f5a5282666a896494a702da3aeb9962357d1fbfeccf98bac3ca02072c6b70e2dc8d8d53d9ca741c868788c
d4b9c7ac3be600dd167a1d6bb612b623812ccbdc877e5d518c5c33a14992cf9b18767c768ea28e12c90089aa9ce392
0c4c4745215f29589705b1ac4cc750a351eba6bbf206a26d1a88c0e292f032aecf81985c08395491cc8b327b39e084
74ba2b91f747d8acba24c0eb83a4a269ea288702d931639b1f7b1008cc186dc206a73b7f374f303702611a1382babc
245fa08d8103e1104067c719601271efb9de3a967e29dcbff21df34fbd06989ce6ce3b21aea0e73d5dc2753fd3ec90
8f58fa04d1c424da8508bca0a7c770ec1fac7fd6db62e859337dda807068fb55fb503795c0c15726301650c210a115
2f78e42d6ca110f548b5aa59f6b11b4081aaee6b55fc0e0ce66c578580c57d178eb13a09b0db78bb82af37234eda37
adc467aec54059bf9f9c2f7b144b1ebcbe0b7e0ed2ee213c611091d505b733839a23ee3a487301a2fdaef7645d3efc
cba588c87f7376f589a28d890531c6277d596defe5363aef58a4d361179876bde107cd6512d3b832cbea523ad9232d
7c29d8ca4a42e71fde3c97256cae02b538a9501a37e13e59990ed68348ff9cc56f75b6e806c4a2e9ab84bf05a58f0f
e4a1980201f5077b9536cd9343375bddc020e2521ef4f05e78db4c8b6fa6e74e7eaf5963774b8b8666997a275a0987
6be15e740220b7cb882077a478184d2ee905edb5d0a0c2f45600751406dcd3e1138d7b8f8acdc65518adc8b36cc640
bf87ad38a2fe83a0983069753b275935fcc050484d4c3fb4a7fb60e65bc1e74b93c4152d82a38bd65d94f39e93ec3e
cd15da6034d0a2d95e3f8a1174ccb8c263e7d661ec745f1127450243c62b445d45cfba20a7d0bc7ed5376291a8f50c
5f2b26b0e3a4ec886950ac4042437afc81134e4d71dc0ac3b897ede2074e6ee290e1673cfeed66c796d5c6b83a858a
4ec15a7abe574c11857eca5de8b78a4192b29e5e0ab8a06c75ac722fd07429a3e588d1e4557b02fdbd56a91949c08a
650e3f7f84878983ee33b86eac1e7aa8b9a9065864bf15191f2be9d2e3c26bebc38129f4150db774056f99423a7a99
1a77ff98c14b4eb61089bdfa6165e887f2bbc03abd69d5833bd441245bebb9c6b0ab747b41cbb350a4609562cfc29b
a83f5087e0b8eae03819af80429094a6a9b8b2e2feb1b01ec48d3a59cc03dcb1dec0b83c64de2001dc6b5c2d3a9d6c
150c14c5c80441157c4d8f3a1b5eea96b408b3ebfdfae0f048423b699a6a19f66664a6903960a7a36de2e176c34279
e78c2745d5f98cc400a8ae0e60fd68dca60b3dd5f3e278fbfdff56181275d13ddbaa8506d56f5276b7174ea12302ac
6f5165eb18855d0a06f2ce1c16e1141083fb9200a575c827722dd9a5361c952d0fbec1eb453674e959e91cd0d8ebe6
36027ca144a8ccaa654e261a0cb284de680c3b8a36224b198ef2884a2ebd326489cb4e7dbd05e43c1180277843947b
02c2bc42838dd9bdb715d93e79e3ae8786c06ff1602d4e5d35a6c60ed08040a764206c57e466460468fe5780b99db4
01812703e3492807e1d337d4c81b8115f2772a3daa81055098f7f9bcd8306a0fe664a274a420bb362feff7ee0a5073
01eabf8981dda8b6972beb52ab4fe61f0da32e054f19893ed36519c1411420daaa5e77ddd3860f434e17826b6b89ea
89cd36901f7c46a43d8ddaef99f15a9a264603fa4f7dfd07edbb459460e5af59ac34be04c04cdfd5bb61203c1f6e39
20b9525ee39a289e1807f93bbc93962bcc754da13044cfaec6be157a26bb9ea7ceed24c44d2bc7b87f0a47f67c3237
41ab414929f29dd98ade35a212db44eb953ff3ec09494f09b3f984e7e32d5c3064f6aa1b45f31c2697f30206ad743e
d1591cae215f39ac444f3aa29f6a8a9eff1b758ae5bcccd872eb7e332f1ea4bff68a23a77c8c4d5080ed2a64876045
c2aaa4fd7348f982dab7f567b45e382b47fe973decd8ffd295d00737ed237a1686717a8294ed44e2879fafa46ef9de
db8f6f01248f33bd143bdcbc3d7c8c2be910193f061ac9ab78095687548538c82237e71f46b946c474c09f4c000000
0000000438

Wynik użycia powyższego ciągu bajtów oraz klucza JWE_MAC_KEY 0fae0202c8aa5d39bac1b9f58a9f440c
w funkcji haszującej HS256 zwraca 32 bajtową wartość w postaci szesnastkowej:

fb1fd818d7ca45d9a59887561bbab110625d28d63a74d28c90d143724dfa3357

wydzielając pierwsze 16 bajtów otrzymanego wyniku:

fb1fd818d7ca45d9a59887561bbab110

po przekodowaniu do formatu Base64URL:

-x_YGNfKRdmlmIdWG7qxEA

otrzymujemy wyliczoną etykietę uwierzytelniającą identyczną z B.5.8a.

B.5.9 Pełna postać obiektu JWE przykładowej komendy przesyłanej z kasy fiskalnej:

eyJraWQiOiIzQTAwMDAwMDA4RTY4RjU1ODE1RDRFQTYzQTAwMDEwMDAwMDAwOCwgQ049ZUthc3ktU3ViQ0EiLCJlbmMiOi
JBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiUlNBMV81In0.giC4C064EjKUdWmh0TmoQVuXbxByz5yWO53Hxda3Je1gRchNmnq0
s38RXyJt9L1e3SDe5hnZuVtgPKufUBgEblItprryumGYnqyhuzIbD0m8akTq9JyJHQ7SERZlGYIzAgQbIn7NJAKswtzhpP
56PxSnMRwegdx0PoW-ZlTx2dYSpHRobWYvpHjz4t25H_poYZh2nAmmzC4nWOGnlshNI0qxk21E64_Tb-
4ACpoqvk6WlPGygUYT4M1hoAN4w_P0fsTyQxcmsXt3RpfiCbCROY2oLyQYGVYnTodbpLp7T4kVKN3XnzT6szBFzMCJsQ9B
0Ug26mQARkH0cx7FWOtVCg.x3NlSpdTUDFhmlJfQoXz3Q.jnYxL4MrKbWmgY5ZeUrL_etV-
byYTeEwp8fH1j5q8ii54kYWQPUBErh3APg7KLl8ZjY644HdbcZgy168x0cACpVhh5MqA93K5CXl0e-
4VUH97iBcHo_VdzUW_iqX3HPyfl1WLrt2PgIiqFOuzjapVYiVFzmXwhKsoWx4oYzIJfUJYM1QFcHnPVWPONlTnpDV6VRss

km3oC4sCn9DW0TJ-
h8HHzvXT18n6F1SHLrqcVgfb4cpz5w6X_k8TBPXaJNgOvEgcbUTXNkKkUWs2xTKNdJAinKTzXR9WFsPajd6R5brwVIEpRg
sHy6icr4RyxGO7fPS8JmKsbEY2CqedVO62ZtYREH1K2giji5lXPEpLPa7kFHdJ4uknjOjbgK-_Kbb9BUVdhdFO6-
bNpT67fiReZ--JLyu-cAYVnoTMj0GqSXOjNLiPZbVG1Q3Q02yw875kPf0nrlPihkNoCGgdBgP66mvF0CdP-
0hoZiMYKh9qOzeAtuiDb0kQL91mPexz_YZ1GQs-UrkYP85Fnv-vpvPkgBp9kJl9x1SiB4qvj86Ryaf-
ic8P_FvOy9bPv9wRtGIaDTcJBuK0vaIb7W7FCYiBKyKv6oR0vsoXghHS8NrH7ARm0VIC-
q9v_S8exfy5Rik6znN51Qwsdz5qG0b-rQU5Gs1hLFckc8Ra1wDMvyfv6qSE6-
dbpmbIsw9rCh2tvNzwM2nN4cHMZQErfpa8-
bTuGcRehZVwrjmfYkV9kcWqbSVajJfWAzeZLmjmcU3hytB6Ke7Yo2HyIjtQNqfWyWY4JmpgqSEVexk6MxeBQr35s2LKZ8H
ouO7jqqPV1RHh_oFIxNcaleisxh4nuEm3T8OfXU8UHvdjRHu2V_HjLZFFtuzT51iydzcHCUVK020mNqF92mMg3w3p6VTe6
xBtteuwIfG5uORdfw9Onu1u3e-PVe7P3H27iuPvLdS-
hG0ywN8aissvnDrIe2gKL_Na7Cuf_9XGv2EHXEEFqYJ67GUiDMYEK1M3JVM0QiQ0zFL1llPwyN9nHdXRyfneWo4931krUe
UYh-yxAtmgeH2lkT67pQ6jwZrqXS9WVBpBdN5JzMS8RjJShZY2BEotJp5MqMdz-
IfZwnx07JBjuMobskg_1yPmtCWQXoAb-MA574jiV40EEKq9HkS27T59wOS-
XdOi32KJHs3a9b1pSgmZqiWSUpwLaOuuZYjV9H7_sz5i6w8oCByxrcOLcjY1T2cp0HIaHiM1LnHrDvmAN0Weh1rthK2I4E
sy9yHfl1RjFwzoUmSz5sYdnx2jqKOEskAiaqc45IMTEdFIV8pWJcFsaxMx1CjUeumu_IGom0aiMDikvAyrs-
BmFwIOVSRzIsyeznghHS6K5H3R9isuiTA64OkomnqKIcC2TFjmx97EAjMGG3CBqc7fzdPMDcCYRoTgrq8JF-
gjYED4RBAZ8cZYBJx77neOpZ-
Kdy_8h3zT70GmJzmzjshrqDnPV3CdT_T7JCPWPoE0cQk2oUIvKCnx3DsH6x_1tti6FkzfdqAcGj7VftQN5XAwVcmMBZQwh
ChFS945C1soRD1SLWqWfaxG0CBqu5rVfwODOZsV4WAxX0XjrE6CbDbeLuCrzcjTto3rcRnrsVAWb-
fnC97FEsevL4Lfg7S7iE8YRCR1QW3M4OaI-46SHMBov2u92RdPvzLpYjIf3N29YmijYkFMcYnfVlt7-
U2Ou9YpNNhF5h2veEHzWUS07gyy-pSOtkjLXwp2MpKQucf3jyXJWyuArU4qVAaN-E-
WZkO1oNI_5zFb3W26AbEoumrhL8FpY8P5KGYAgH1B3uVNs2TQzdb3cAg4lIe9PBeeNtMi2-m505-
r1ljd0uLhmaZeidaCYdr4V50AiC3y4ggd6R4GE0u6QXttdCgwvRWAHUUBtzT4RONe4-KzcZVGK3Is2zGQL-
HrTii_oOgmDBpdTsnWTX8wFBITUw_tKf7YOZbwedLk8QVLYKji9ZdlPOek-w-
zRXaYDTQotleP4oRdMy4wmPn1mHsdF8RJ0UCQ8YrRF1Fz7ogp9C8ftU3YpGo9QxfKyaw46TsiGlQrEBCQ3r8gRNOTXHcCs
O4l-3iB05u4pDhZzz-7WbHltXGuDqFik7BWnq-
V0wRhX7KXei3ikGSsp5eCrigbHWsci_QdCmj5YjR5FV7Av29VqkZScCKZQ4_f4SHiYPuM7hurB56qLmpBlhkvxUZHyvp0u
PCa-vDgSn0FQ23dAVvmUI6epkad_-YwUtOthCJvfphZeiH8rvAOr1p1YM71EEkW-
u5xrCrdHtBy7NQpGCVYs_Cm6g_UIfguOrgOBmvgEKQlKapuLLi_rGwHsSNOlnMA9yx3sC4PGTeIAHca1wtOp1sFQwUxcgE
QRV8TY86G17qlrQIs-v9-
uDwSEI7aZpqGfZmZKaQOWCno23i4XbDQnnnjCdF1fmMxACorg5g_Wjcpgs91fPiePv9_1YYEnXRPduqhQbVb1J2txdOoSM
CrG9RZesYhV0KBvLOHBbhFBCD-
5IApXXIJ3It2aU2HJUtD77B60U2dOlZ6RzQ2OvmNgJ8oUSozKplTiYaDLKE3mgMO4o2IksZjvKISi69MmSJy059vQXkPBG
AJ3hDlHsCwrxCg43ZvbcV2T55466HhsBv8WAtTl01psYO0IBAp2QgbFfkZkYEaP5XgLmdtAGBJwPjSSgH4dM31MgbgRXyd
yo9qoEFUJj3-bzYMGoP5mSidKQguzYv7_fuClBzAeq_iYHdqLaXK-tSq0_mHw2jLgVPGYk-
02UZwUEUINqqXnfd04YPQ04XgmtrieqJzTaQH3xGpD2N2u-Z8VqaJkYD-
k99_Qftu0WUYOWvWaw0vgTATN_Vu2EgPB9uOSC5Ul7jmiieGAf5O7yTlivMdU2hMETPrsa-
FXomu56nzu0kxE0rx7h_Ckf2fDI3QatBSSnyndmK3jWiEttE65U_8-wJSU8Js_mE5-
MtXDBk9qobRfMcJpfzAgatdD7RWRyuIV85rERPOqKfaoqe_xt1iuW8zNhy634zLx6kv_aKI6d8jE1QgO0qZIdgRcKqpP1z
SPmC2rf1Z7ReOCtH_pc97Nj_0pXQBzftI3oWhnF6gpTtROKHn6-kbvne249vASSPM70UO9y8PXyMK-
kQGT8GGsmreAlWh1SFOMgiN-cfRrlGxHTAn0w.-x_YGNfKRdmlmIdWG7qxEA

Załącznik C

C.1 Przykładowe certyfikaty środowiska testowego kas w postaci oprogramowania

C.1.1 Certyfikat klucza publicznego ministerstwa do podpisywania komend oraz szyfrowania klucza szyfrującego przesyłanych danych oraz dokumentów z kasy fiskalnej do repozytorium:

```
-----BEGIN CERTIFICATE-----
MIIFHDCCAwSgAwIBAgITOgAAAAjmj1WBXU6mOgABAAAACDANBgkqhkiG9w0BAQ0F
ADAWMRQwEgYDVQQDEwtlS2FzeS1TdWJDQTAgFw0xNzA4MjIwNjMzMTNaGA8yMDky
MDcxMDEyMjcyOVowgcgxCzAJBgNVBAYTAlBMMRQwEgYDVQQIEwtNYXpvd2llY2tp
ZTERMA8GA1UEBxMIV2Fyc3phd2ExHzAdBgNVBAoMFk1pbmlzdGVyc3R3byBGaW5h
bnPDs3cxIzAhBgNVBAsTGkRlcGFydGFtZW50IEluZm9ybWF0eXphY2ppMR4wHAYD
VQQDExV0ZXN0LWUta2FzeS5tZi5nb3YucGwxKjAoBgkqhkiG9w0BCQEWG2luZm8u
ZS1kZWtsYXJhY2plQG1mLmdvdi5wbDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMvyVXGj8YNhy6P28bKj9MleA7+QXKCtPJZ4M6MIxiaqA4lodd9No+Ws
gRETVzEPiB8raL9n3uM+RBFwK2A4VvuAWuGZx2drkfMZnpSVFLOsQnadB1rjBCY5
G/pMX6eI7Bltx4XFYK/1cY1U+mFVc94Ryfyxyy0ZWSD8IGV9n0AilDpRfIJBOu5a
3oquz8ZZGuWyU95KWBKRAD7SV2bpTlYWX4UHhTe323HTYL3rDbKP73HAoylObSmS
vmB9MyNzWgBf73UOHmzXPqpuRbLFnR+llTA0FA8kOylxtijygMXpICOai7av2ofG
t65v0GJg5wlJuqWvkQXFUyoyGGUYaQsCAwEAAaOBrTCBqjAdBgNVHQ4EFgQUx7xK
j1TXCorOExa2hY/jdz6NkA0wHwYDVR0jBBgwFoAUBb+Partd6TV4PV1kTUrtJads
SdowWgYIKwYBBQUHAQEETjBMMEoGCCsGAQUFBzAChj5maWxlOi8vLy9zYXAtd2lu
LTgyNi9DZXJ0RW5yb2xsL3NhcC13aW4tODI2X2VLYXN5LVN1YkNBKDEpLmNydDAM
BgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBDQUAA4ICAQCkdUR2DhgiexUW+y2rgaE6
orWBPyMxveH2IPv0rPGzqdgUFcNH816YzDorEnOAvbRLB8BaoH+Wn/eElAQxqE5+
47VgScIUF4oNHwXnnflR1XRoYcFZ/fBkIW2nfOK1C8y2vHtZG1QEyyVD/cxv7ubg
OiJfOYScsHv5DItStFUBclvg3xrFi2zG5ahblMwqCGrvgPKOxR9+mXGD+eoThBHE
P6aJF3Zu41mVwT/4cbSr5m3c77deEQ2CpQPGL874PiHy9omkjev9F5yoBzI7ypha
lyEIdbASU0UiUErjbS+hnw0RErV1bQQzQfS7qiKMBZTM4pzOv/Ro6f+OcBf7c16X
tHrEgli/aNagKo34nFhUscQcUTCh3MsCKuVSZU3dbCdSLIvdoJIS5FLP+gr8LbQW
9uR/NgwJhYr/w06k6AOF+TaJw8eakv5ELDOuzhipqB63BuMSCGFZcUQ2bDhdc5gc
V9GlNgVEXmToee3fn89OQTC7GrCwFzNxwAM6gJ0MARyWl5Hmgr/pOb1MX5Vehgao
HpjoveMAacONbtiOwfMUyhPdCJmnLP67lokvGq7PDJ/DUbespAqVm91TM6QbWjda
nKGB6kJY+7H5ESI8sp/nzjHXdZxeIPO7lOTItKdRW82kRcBR9TNDSS6rt5sI16LW
0NCJ2zprYt8XrNO728ljyA==
-----END CERTIFICATE-----
```

C.1.2 Certyfikat klucza publicznego kasy fiskalnej do podpisywania danych wytworzonych przez kasę oraz szyfrowania klucza szyfrującego przesyłanych komend wysyłanych do kasy:

```
-----BEGIN CERTIFICATE-----
MIIDKjCCApOgAwIBAgIQ27uolIpDHKdAJjLSAHD4+zANBgkqhkiG9w0BAQsFADAU
MRIwEAYDVQQDEwlNRiBlLUthc3kwHhcNMjAwMzE2MTAzNTU5WhcNMjUwMzE2MTAz
NTU4WjCBrjEjMCEGA1UECxMaRGVwYXJ0YW1lbnQgSW5mb3JtYXR5emFjamkxHjAc
BgNVBAoTFU1pbmlzdGVyc3R3byBGaW5hbnNvdzEZMBcGA1UEBRMQVkFUUEwtNjk3
MDAwMDgwMjEWMBQGA1UEAxMNV1RFMjAwMTAwMDAwOTERMA8GA1UEBxMIV2Fyc3ph
d2ExFDASBgNVBAgTC01hem93aWVja2llMQswCQYDVQQGEwJQTDCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALtSH7AwSOT4qT863BAwbt2DvGqEgDNV/g0d
tWK81C5vK677mb9Y7U0PccRJG4ht7B+kmRvfsO92YgnjmpQEqAJj4GyCicGXaI+6
f6xeUQknwvpAHvpmPGvZjlsAmHyScLdGqOXzQgrxV/WE64jJgendcucsGu6AZHRC
W7rxGMAxGA2ySgEpNZBQq8hphl7sAjj0PHZCJwU5PP1nsNzddSOEJndJYHNbbrom
6ZFLbju2QMk/gWpFACgYV9hoHiOo7BCSiZ3fPC4tpmhxOPqmdZDYwInSU0MgaYP3
p803z2f16g1kg2Tldt4GroubKiffW4RumFwuIPZZe8DKD834PQ8CAwEAAaNeMFww
EwYDVR0lBAwwCgYIKwYBBQUHAwIwRQYDVR0BBD4wPIAQxg+n+j1jAU1f23nuS65X
PaEWMBQxEjAQBgNVBAMTCU1GIGUtS2FzeYIQs8LVeZ9uP5lAlnvXe8bYejANBgkq
hkiG9w0BAQsFAAOBgQBZfk/KxEy/3zIfP0r4Nt5Dg5LbJ737kRfIZRhu3PHmMthA
ac2kTLtaaaWC+iL70nm8t/J9kRD9Uyk83vLmLbPGVEbcOlY+5Oo5XYetubSdLFnL
m4kiFUDh5NP4AKzQdTpCp4jbAOWRFJCbrZZbV6M0XytAE/mlrTrml9K313MxRw==
-----END CERTIFICATE-----
```

C.2 Przykładowe dane procesu podpisywania danych kas w postaci oprogramowania

C.2.1 Przykładowe zbiory danych

C.2.1a Pełna postać przykładowego zbioru danych:


```
{"JPK":{"naglowek":{"wersja":"JPK_KASA_v2-0","wysylka":"Z","dataJPK":"2020-04-
10T10:23:45.678Z"},"podmiot1":{"nazwaPod":"Nazwa
podmiotu","nrFabr":"WTE2001000009","NIP":"6970000802","adresPod":{"ulica":"Ulica","miejsc":"Mi
ejscowosc","nrLok":"NrLok","poczta":"Poczta","nrDomu":"NrDomu","kodPoczt":"00-
000"},"nrUnik":"WTE2001000009","nrEwid":"2020/000001949"},"content":[{"rapFisk":{"zakRap":"202
0-04-
10T01:23:45.789Z","firmwareId":"01","sumaZm":"9DD845A0C9C285DC2E13F3253352E1836DC603C0","typWl
asn":"1","kodUS":"3014","serwID":"KW123","pamiecChr":1,"sposobUzytk":"4","licznikParag":1,"JPK
ID":1,"dataFisk":"2020-04-
10T01:23:45.678Z","kasjer":"Kasjer","stPTU":[{"id":"A","wart":2300},{"id":"B","wart":800},{"id
":"C","wart":500},{"id":"D","wart":0},{"id":"E","wart":0},{"id":"F","wart":0},{"id":"G","wart"
:"ZW"}],"model":"PREFIX DLA TESTÓW
KW","waluta":"PLN","katKasy":["01"],"nrDok":1,"nrKasy":"001","podpis":{"RSA":"3019505879124143
c92b60d5e57ebc08ba8fb7c9d2ce1bae02ba6b77a9c14b7794f7f8acbddff2c2e382fbb6820cd0e0a87fa988f2c67f
9b34ae0571cfc0b23b727b7912c9d30b567c56e710cbfa88f09937bbfd1c54065df893eafb7455823716c292d548dc
98dfc4ad29c81332450b84bea1a4bbf11e0c4dcc8d21f835476b87ff5a68be7d514fe15d3ebb76c2559bfe93a8cdfd
09bf9bab7b5df918225c2f46778f59fb9deef898eb4e932f405a1403d9e0e78772c25675f14edc34d457f42aeb0a71
9a7a9638654bae7823641b1f95981b37fbd2cff3fda256e2e8f2e5aa8aca729e2d9a9b32893d6664b223da5c1879af
cec64fea8b11fe22a622de55bb"}}},{"zdarzenie":{"pamiecChr":1,"JPKID":2,"dataCzas":"2020-04-
10T02:23:45.678Z","typ":{"21":{"atrybuty":{"checkFreqWebApi":100,"sendFreqEventHub":100,"shipp
mentType":"RF"},"info":"Zapis harmonogramu transmisji danych w bazie danych
kasy"}}}},{"wydrNiefisk":{"pamiecChr":1,"zak":"2020-04-
10T03:23:45.678Z","JPKID":3,"kasjer":"Kasjer","grafika":1,"nrDok":2,"zawart":[{"kodGraficzny":
"kodGraficzny0","kodKreskowy":"kodKreskowy0","tekst":"tekst0"},{"kodGraficzny":["kodGraficzny1
","kodGraficzny2"],"kodKreskowy":["kodKreskowy1","kodKreskowy2"],"tekst":["WYDRUK
NIEFISKALNY","TEST"]}],"nrKasy":"001","podpis":{"RSA":"282f2b77102bbb60717093d6ad9c2db648201be
698baa316c03e7598446fc7915042e9d4a19d5a846ad5998c7467ecedd1f545dc6619d6c0a17e55f9380d01e584dff
a84971bc9e91f922e6f2f4fe243c1382b8fa06780945124199262 2faa9e7b83feb4a3d6d8f742278c1e5174570a63b
113495384a346ad6f1e0f5072d91c9227ea68abbbc9a902f0463a126fbb43ef1380dac8421cd8d45cb797ab75a7c3b
08988709e64bc174d9aeead5e9ea1a44d01e0c3e0a7ecb97baec560f34f4a6ce34d27749d5b220384ce2d9add085e7
7a947be2b532c555ce0f5a92b9266cc262580ce7d56c528792d5a908b8a503b4188e3e77f3230cb53fc5e1cbba9c79
fb1"}}},{"paragAnul":{"pamiecChr":1,"total":{"zaplZwrot":1000000},"zakSprzed":"2020-04-
10T06:23:45.678Z","JPKID":6,"nrParag":3,"kasjer":"Kasjer","stPTU":[{"id":"G","wart":"ZW"}],"po
dsum":{"waluta":"PLN","sumaNetto":[{"brutto":1000000,"vat":0,"idStPTU":"G"}],"sumaBrutto":1000
000,"sumaPod":1000000},"nrDok":5,"pozycja":[{"towar":{"brutto":1000000,"ilosc":"1","oper":fals
e,"cena":1000000,"nazwa":"Nazwa
towaru","idStPTU":"G"}}],"nrKasy":"001","podpis":{"RSA":"9e61a538a24334c0af624987d5967c11d8928
6f02bcd1c9123ff284c460e3dcf2ae7cca47c1a5079010b201d2a6ace3c1d619377c57501a3773e7faaa3ac3c2ea7e
b26409b3ff852d715cf1c16cc1b490e7876bc23af51720174c729a2c8aea7d4a58cf3d99b54582698764e58922af46
9d011cbc5100bb57bbbcf3f373bf629a33257eec641662c3f44cbc9d39c7d7f885a1b8fcd6da954e918077f7ff3279
e2f84ea9aa944ab9123dd10f711870a8d1d6856ecaa6a6df0a7bce1703fd79376bec82cec37ea4ba48a64063ebcdf4
d99f9e18c37d0777bd4437ca819d19b2a8b2f73cff076cb240ee0580d90eaba0c7aad3dff10af58e64c03e51453caa
1c8f3","JPK":"000000000000000000","SHA":"eee0e3068482a34527630f4c73c05d0d3523899f5fa25d022b941
5ff8057d3be"}}},{"paragAnul":{"pamiecChr":1,"total":{"zaplZwrot":10000000},"zakSprzed":"2020-
04-
10T09:23:45.678Z","JPKID":9,"nrParag":6,"kasjer":"Kasjer","stPTU":[{"id":"G","wart":"ZW"}],"po
dsum":{"waluta":"PLN","sumaNetto":[{"brutto":10000000,"vat":0,"idStPTU":"G"}],"sumaBrutto":100
00000,"sumaPod":10000000},"nrDok":8,"pozycja":[{"towar":{"brutto":10000000,"ilosc":"1","oper":
false,"cena":10000000,"nazwa":"Nazwa
towaru","idStPTU":"G"}}],"nrKasy":"001","podpis":{"RSA":"ab6c66f6f3cbc34dde1e8f3b3080bee64555a
b5f3886bae21f4be9139a11f6c09bc8765f229bfd99bece7fb7dbb5cf18ffc17e7cfbd56bc8b637d4a821e483d8b6c
5cc947e356a543b5eba1020a499fe7506d49c5d3fbdb61dbd428124783fe0ee6532f57b7600d8266435eda9e5fead4
7c4d31b18961fe21ad824ccc6b20d51961a6221bcef4554322f3127c9e488aaf6a54d0498096484840668372b5cf6b
22a73a26334249a74fb4c87568dbde4693dfeed4ec44f473dcf4921c3da287f3e8b1085521a833b416c7a269fa6d03
e1d23ea1fde9577c78ae60179b4303629674f1fdfbacaed55706a7b466957b93c083d1e3f4af231f503cdb694b9afb
0ebf3","JPK":"001000000000000006","SHA":"a64a913986f2a18d4db5ecbe02309fc96d19c683830622140a2d4
310425f911c"}}},{"paragAnul":{"pamiecChr":1,"total":{"zaplZwrot":100000000},"zakSprzed":"2020-
04-
10T10:23:45.678Z","JPKID":10,"nrParag":7,"kasjer":"Kasjer","stPTU":[{"id":"G","wart":"ZW"}],"p
odsum":{"waluta":"PLN","sumaNetto":[{"brutto":100000000,"vat":0,"idStPTU":"G"}],"sumaBrutto":1
00000000,"sumaPod":100000000},"nrDok":9,"pozycja":[{"towar":{"brutto":100000000,"ilosc":"1","o
```

per":false,"cena":100000000,"nazwa":"Nazwa
towaru","idStPTU":"G"}}],"nrKasy":"001","podpis":{"RSA":"54ce7bad1079bc8a7a69908766aa6e420edf6
11442f28f28cfbd51c3c181ad54505ff81465ab6dbbd93fcaf0fb78b83ef56304e83fb302bf0e07c2114b7a947ad20
c012d204efe1cd53aaff0469830aabe01a8a5828c798872bd6dbb7d8767ab832d892a40f81c07d7246e34f8716d5cd
0fd206da3bbb89aae831010f3e2278a6ce76c9206b022e6a246a0b889cbe571c062bf214a3dd924168f4913bde545d
ba76f42875bb1c7060fd06ded94f9c9ab7e9f2d04f276b9ccfaebdbdac48cc92b5b4f629504daca05d887a1cd8e035
e50d7b07af374609f3bd6080e4bed80330d62924987d440f0b06f7e99a3ec980df0e1951e073854e20173a937ec2f1
ca93f","JPK":"0010000000000000009","SHA":"ac6450833bef0f47888dea1272d179e8a197c8b6968c16782eeaf
f4f2769430d"}}},{"rapDob":{"sprzedBrutto":49060,"zakSprzed":"2020-04-
10T22:23:45.678Z","liczbaParAnul":3,"zakRap":"2020-04-
10T23:23:45.678Z","sprzedPar":{"wartWgPTU":[{"netto":22000,"vat":5060,"idStPTU":"A"},{"netto":
20200,"vat":0,"idStPTU":"G"}],"sumaBrutto":49060,"sumaPod":5060},"podatekNal":5060,"dokNiefisk
":1,"liczbaPar":4,"pamiecChr":1,"JPKID":11,"kasjer":"Kasjer","stPTU":[{"id":"A","wart":2300},{
"id":"G","wart":"ZW"}],"waluta":"PLN","wartParAnul":111000000,"rozpSprzed":"2020-04-
10T04:23:45.678Z","nrDok":10,"nrRap":1,"nrKasy":"001","podpis":{"RSA":"21184e6e94b7c822223c90b
3769567188c285c262d10be052c6820242368a5f655af1c77138930fe51873f2e2eea6c6a7666f3f8cf9f1776dad23
ce32afb687f6b5057bdf38ce3bb732ff27d95b1682c541b43410af8cad7262bc93dc7466b09588311242b4c297251a
e54afd8911607a482854a8bb326b68ae7c8d1295266488ee635a483e90157f8c943a3add99329edbc2ca18d9954e97
6f32f4bda9d74eb99527f411436c8857d4b8e804e72b0c0e6a58e47a6975749b8421874f095041cc5429d9d18b3f44
6f0c834964e2150c2f56b6de9e72f62cfa5f194aa5650a55b64f5f903d52b9435e84183860810835e5a266aef281b9
2ab8a257d9467f4c1ce","JPK":"0000000000000000000","SHA":"7d68d863163c76b46d26e543d44d0f7d373beef
55d055f3ffb929484d9e374f4"}}}]}}

C.2.1b Ustrukturyzowana postać przykładowego zbioru danych:


```
{
    "JPK": {
        "naglowek": {
            "wersja": "JPK_KASA_v2-0",
            "dataJPK": "2020-04-10T10:23:45.678Z",
            "wysylka": "Z"
        },
        "podmiot1": {
            "nazwaPod": "Nazwa podmiotu",
            "nrFabr": "WTE2001000009",
            "NIP": "6970000802",
            "adresPod": {
                "ulica": "Ulica",
                "miejsc": "Miejscowosc",
                "nrLok": "NrLok",
                "poczta": "Poczta",
                "nrDomu": "NrDomu",
                "kodPoczt": "00-000"
            },
            "nrUnik": "WTE2001000009",
            "nrEwid": "2020/000001949"
        },
        "content": [
            {
                "rapFisk": {
                    "JPKID": 1,
                    "pamiecChr": 1,
                    "nrDok": 1,
                    "dataFisk": "2020-04-10T01:23:45.678Z",
                    "stPTU": [
                        {
                            "id": "A",
                            "wart": 2300
                        },
                        {
                            "id": "B",
                            "wart": 800
                        },
                        {
                            "id": "C",
                            "wart": 500
                        },
                        {
                            "id": "D",
                            "wart": 0
```

```
                        },
                        {
                            "id": "E",
                            "wart": 0
                        },
                        {
                            "id": "F",
                            "wart": 0
                        },
                        {
                            "id": "G",
                            "wart": "ZW"
                        }
                    ],
                    "katKasy": [
                        "01"
                    ],
                    "licznikParag": 1,
                    "model": "PREFIX DLA TESTÓW KW",
                    "typWlasn": "1",
                    "sposobUzytk": "4",
                    "firmwareId": "01",
                    "sumaZm": "9DD845A0C9C285DC2E13F3253352E1836DC603C0",
                    "kodUS": "3014",
                    "serwID": "KW123",
                    "waluta": "PLN",
                    "nrKasy": "001",
                    "kasjer": "Kasjer",
                    "zakRap": "2020-04-10T01:23:45.789Z",
                    "podpis": {
                        "RSA":
"3019505879124143c92b60d5e57ebc08ba8fb7c9d2ce1bae02ba6b77a9c14b7794f7f8acbddff2c2e382fbb6820cd
0e0a87fa988f2c67f9b34ae0571cfc0b23b727b7912c9d30b567c56e710cbfa88f09937bbfd1c54065df893eafb745
5823716c292d548dc98dfc4ad29c81332450b84bea1a4bbf11e0c4dcc8d21f835476b87ff5a68be7d514fe15d3ebb7
6c2559bfe93a8cdfd09bf9bab7b5df918225c2f46778f59fb9deef898eb4e932f405a1403d9e0e78772c25675f14ed
c34d457f42aeb0a719a7a9638654bae7823641b1f95981b37fbd2cff3fda256e2e8f2e5aa8aca729e2d9a9b32893d6
664b223da5c1879afcec64fea8b11fe22a622de55bb"
                    }
                }
            },
            {
                "zdarzenie": {
                    "JPKID": 2,
                    "pamiecChr": 1,
                    "dataCzas": "2020-04-10T02:23:45.678Z",
                    "typ": {
                        "21": {
                            "info": "Zapis harmonogramu transmisji danych w bazie danych
kasy",
                            "atrybuty": {
                                "sendFreqEventHub": 100,
                                "checkFreqWebApi": 100,
                                "shippmentType": "RF"
                            }
                        }
                    }
                }
            },
            {
                "wydrNiefisk": {
                    "JPKID": 3,
                    "pamiecChr": 1,
                    "grafika": 1,
                    "nrDok": 2,
                    "zawart": [
                        {
                            "kodGraficzny": "kodGraficzny0",
                            "kodKreskowy": "kodKreskowy0",
                            "tekst": "tekst0"
                        },
                        {
```

```
                            "tekst": [
                                "WYDRUK NIEFISKALNY",
                                "TEST"
                            ],
                            "kodKreskowy": [
                                "kodKreskowy1",
                                "kodKreskowy2"
                            ],
                            "kodGraficzny": [
                                "kodGraficzny1",
                                "kodGraficzny2"
                            ]
                        }
                    ],
                    "zak": "2020-04-10T03:23:45.678Z",
                    "nrKasy": "001",
                    "kasjer": "Kasjer",
                    "podpis": {
                        "RSA":
"282f2b77102bbb60717093d6ad9c2db648201be698baa316c03e7598446fc7915042e9d4a19d5a846ad5998c7467e
cedd1f545dc6619d6c0a17e55f9380d01e584dffa84971bc9e91f922e6f2f4fe243c1382b8fa067809451241992622
faa9e7b83feb4a3d6d8f742278c1e5174570a63b113495384a346ad6f1e0f5072d91c9227ea68abbbc9a902f0463a1
26fbb43ef1380dac8421cd8d45cb797ab75a7c3b08988709e64bc174d9aeead5e9ea1a44d01e0c3e0a7ecb97baec56
0f34f4a6ce34d27749d5b220384ce2d9add085e77a947be2b532c555ce0f5a92b9266cc262580ce7d56c528792d5a9
08b8a503b4188e3e77f3230cb53fc5e1cbba9c79fb1"
                    }
                }
            },
            {
                "paragAnul": {
                    "JPKID": 6,
                    "pamiecChr": 1,
                    "nrDok": 5,
                    "pozycja": [
                        {
                            "towar": {
                                "brutto": 1000000,
                                "cena": 1000000,
                                "idStPTU": "G",
                                "ilosc": "1",
                                "nazwa": "Nazwa towaru",
                                "oper": false
                            }
                        }
                    ],
                    "stPTU": [
                        {
                            "id": "G",
                            "wart": "ZW"
                        }
                    ],
                    "podsum": {
                        "sumaNetto": [
                            {
                                "idStPTU": "G",
                                "brutto": 1000000,
                                "vat": 0
                            }
                        ],
                        "sumaPod": 1000000,
                        "sumaBrutto": 1000000,
                        "waluta": "PLN"
                    },
                    "total": {
                        "zaplZwrot": 1000000
                    },
                    "nrParag": 3,
                    "nrKasy": "001",
                    "zakSprzed": "2020-04-10T06:23:45.678Z",
                    "kasjer": "Kasjer",
                    "podpis": {
```

```
                        "RSA":
"9e61a538a24334c0af624987d5967c11d89286f02bcd1c9123ff284c460e3dcf2ae7cca47c1a5079010b201d2a6ac
e3c1d619377c57501a3773e7faaa3ac3c2ea7eb26409b3ff852d715cf1c16cc1b490e7876bc23af51720174c729a2c
8aea7d4a58cf3d99b54582698764e58922af469d011cbc5100bb57bbbcf3f373bf629a33257eec641662c3f44cbc9d
39c7d7f885a1b8fcd6da954e918077f7ff3279e2f84ea9aa944ab9123dd10f711870a8d1d6856ecaa6a6df0a7bce17
03fd79376bec82cec37ea4ba48a64063ebcdf4d99f9e18c37d0777bd4437ca819d19b2a8b2f73cff076cb240ee0580
d90eaba0c7aad3dff10af58e64c03e51453caa1c8f3",
                        "SHA":
"eee0e3068482a34527630f4c73c05d0d3523899f5fa25d022b9415ff8057d3be",
                        "JPK": "000000000000000000"
                    }
                }
            },
            {
                "paragAnul": {
                    "JPKID": 9,
                    "pamiecChr": 1,
                    "nrDok": 8,
                    "pozycja": [
                        {
                            "towar": {
                                "brutto": 10000000,
                                "cena": 10000000,
                                "idStPTU": "G",
                                "ilosc": "1",
                                "nazwa": "Nazwa towaru",
                                "oper": false
                            }
                        }
                    ],
                    "stPTU": [
                        {
                            "id": "G",
                            "wart": "ZW"
                        }
                    ],
                    "podsum": {
                        "sumaNetto": [
                            {
                                "idStPTU": "G",
                                "brutto": 10000000,
                                "vat": 0
                            }
                        ],
                        "sumaPod": 10000000,
                        "sumaBrutto": 10000000,
                        "waluta": "PLN"
                    },
                    "total": {
                        "zaplZwrot": 10000000
                    },
                    "nrParag": 6,
                    "nrKasy": "001",
                    "zakSprzed": "2020-04-10T09:23:45.678Z",
                    "kasjer": "Kasjer",
                    "podpis": {
                        "RSA":
"ab6c66f6f3cbc34dde1e8f3b3080bee64555ab5f3886bae21f4be9139a11f6c09bc8765f229bfd99bece7fb7dbb5c
f18ffc17e7cfbd56bc8b637d4a821e483d8b6c5cc947e356a543b5eba1020a499fe7506d49c5d3fbdb61dbd4281247
83fe0ee6532f57b7600d8266435eda9e5fead47c4d31b18961fe21ad824ccc6b20d51961a6221bcef4554322f3127c
9e488aaf6a54d0498096484840668372b5cf6b22a73a26334249a74fb4c87568dbde4693dfeed4ec44f473dcf4921c
3da287f3e8b1085521a833b416c7a269fa6d03e1d23ea1fde9577c78ae60179b4303629674f1fdfbacaed55706a7b4
66957b93c083d1e3f4af231f503cdb694b9afb0ebf3",
                        "SHA":
"a64a913986f2a18d4db5ecbe02309fc96d19c683830622140a2d4310425f911c",
                        "JPK": "0010000000000000006"
                    }
                }
            },
            {
                "paragAnul": {
```

```
                    "JPKID": 10,
                    "pamiecChr": 1,
                    "nrDok": 9,
                    "pozycja": [
                        {
                            "towar": {
                                "brutto": 100000000,
                                "cena": 100000000,
                                "idStPTU": "G",
                                "ilosc": "1",
                                "nazwa": "Nazwa towaru",
                                "oper": false
                            }
                        }
                    ],
                    "stPTU": [
                        {
                            "id": "G",
                            "wart": "ZW"
                        }
                    ],
                    "podsum": {
                        "sumaNetto": [
                            {
                                "idStPTU": "G",
                                "brutto": 100000000,
                                "vat": 0
                            }
                        ],
                        "sumaPod": 100000000,
                        "sumaBrutto": 100000000,
                        "waluta": "PLN"
                    },
                    "total": {
                        "zaplZwrot": 100000000
                    },
                    "nrParag": 7,
                    "nrKasy": "001",
                    "zakSprzed": "2020-04-10T10:23:45.678Z",
                    "kasjer": "Kasjer",
                    "podpis": {
                        "RSA":
"54ce7bad1079bc8a7a69908766aa6e420edf611442f28f28cfbd51c3c181ad54505ff81465ab6dbbd93fcaf0fb78b
83ef56304e83fb302bf0e07c2114b7a947ad20c012d204efe1cd53aaff0469830aabe01a8a5828c798872bd6dbb7d8
767ab832d892a40f81c07d7246e34f8716d5cd0fd206da3bbb89aae831010f3e2278a6ce76c9206b022e6a246a0b88
9cbe571c062bf214a3dd924168f4913bde545dba76f42875bb1c7060fd06ded94f9c9ab7e9f2d04f276b9ccfaebdbd
ac48cc92b5b4f629504daca05d887a1cd8e035e50d7b07af374609f3bd6080e4bed80330d62924987d440f0b06f7e9
9a3ec980df0e1951e073854e20173a937ec2f1ca93f",
                        "SHA":
"ac6450833bef0f47888dea1272d179e8a197c8b6968c16782eeaff4f2769430d",
                        "JPK": "0010000000000000009"
                    }
                }
            },
            {
                "rapDob": {
                    "JPKID": 11,
                    "pamiecChr": 1,
                    "nrDok": 10,
                    "nrRap": 1,
                    "rozpSprzed": "2020-04-10T04:23:45.678Z",
                    "zakSprzed": "2020-04-10T22:23:45.678Z",
                    "stPTU": [
                        {
                            "id": "A",
                            "wart": 2300
                        },
                        {
                            "id": "G",
                            "wart": "ZW"
                        }
```

```
                    ],
                    "sprzedPar": {
                        "sumaBrutto": 49060,
                        "sumaPod": 5060,
                        "wartWgPTU": [
                            {
                                "idStPTU": "A",
                                "netto": 22000,
                                "vat": 5060
                            },
                            {
                                "idStPTU": "G",
                                "netto": 20200,
                                "vat": 0
                            }
                        ]
                    },
                    "podatekNal": 5060,
                    "sprzedBrutto": 49060,
                    "waluta": "PLN",
                    "liczbaPar": 4,
                    "liczbaParAnul": 3,
                    "wartParAnul": 111000000,
                    "dokNiefisk": 1,
                    "zakRap": "2020-04-10T23:23:45.678Z",
                    "nrKasy": "001",
                    "kasjer": "Kasjer",
                    "podpis": {
                        "RSA":
"21184e6e94b7c822223c90b3769567188c285c262d10be052c6820242368a5f655af1c77138930fe51873f2e2eea6
c6a7666f3f8cf9f1776dad23ce32afb687f6b5057bdf38ce3bb732ff27d95b1682c541b43410af8cad7262bc93dc74
66b09588311242b4c297251ae54afd8911607a482854a8bb326b68ae7c8d1295266488ee635a483e90157f8c943a3a
dd99329edbc2ca18d9954e976f32f4bda9d74eb99527f411436c8857d4b8e804e72b0c0e6a58e47a6975749b842187
4f095041cc5429d9d18b3f446f0c834964e2150c2f56b6de9e72f62cfa5f194aa5650a55b64f5f903d52b9435e8418
3860810835e5a266aef281b92ab8a257d9467f4c1ce",
                        "SHA":
"7d68d863163c76b46d26e543d44d0f7d373beef55d055f3ffb929484d9e374f4",
                        "JPK": "000000000000000000"
                    }
                }
            }
        ]
    }
}
```


C.2.2 Przykłady ustrukturyzowanych dokumentów przesyłanych w zbiorach danych:

C.2.2a Ustrukturyzowana postać przykładowego raportu fiskalnego fiskalizacji:


```
{
    "rapFisk": {
        "JPKID": 1,
        "pamiecChr": 1,
        "nrDok": 1,
        "dataFisk": "2020-04-10T01:23:45.678Z",
        "stPTU": [
            {
                "id": "A",
                "wart": 2300
            },
            {
                "id": "B",
                "wart": 800
            },
            {
                "id": "C",
                "wart": 500
            },
```

```
            {
                "id": "D",
                "wart": 0
            },
            {
                "id": "E",
                "wart": 0
            },
            {
                "id": "F",
                "wart": 0
            },
            {
                "id": "G",
                "wart": "ZW"
            }
        ],
        "katKasy": [
            "01"
        ],
        "licznikParag": 1,
        "model": "PREFIX DLA TESTÓW KW",
        "typWlasn": "1",
        "sposobUzytk": "4",
        "firmwareId": "01",
        "sumaZm": "9DD845A0C9C285DC2E13F3253352E1836DC603C0",
        "kodUS": "3014",
        "serwID": "KW123",
        "waluta": "PLN",
        "nrKasy": "001",
        "kasjer": "Kasjer",
        "zakRap": "2020-04-10T01:23:45.789Z",
        "podpis": {
            "RSA":
"3019505879124143c92b60d5e57ebc08ba8fb7c9d2ce1bae02ba6b77a9c14b7794f7f8acbddff2c2e382fbb6820cd
0e0a87fa988f2c67f9b34ae0571cfc0b23b727b7912c9d30b567c56e710cbfa88f09937bbfd1c54065df893eafb745
5823716c292d548dc98dfc4ad29c81332450b84bea1a4bbf11e0c4dcc8d21f835476b87ff5a68be7d514fe15d3ebb7
6c2559bfe93a8cdfd09bf9bab7b5df918225c2f46778f59fb9deef898eb4e932f405a1403d9e0e78772c25675f14ed
c34d457f42aeb0a719a7a9638654bae7823641b1f95981b37fbd2cff3fda256e2e8f2e5aa8aca729e2d9a9b32893d6
664b223da5c1879afcec64fea8b11fe22a622de55bb"
        }
    }
}
```


C.2.2b Ustrukturyzowana postać przykładowego raportu fiskalnego dobowego:


```
{
    "rapDob": {
        "JPKID": 11,
        "pamiecChr": 1,
        "nrDok": 10,
        "nrRap": 1,
        "rozpSprzed": "2020-04-10T04:23:45.678Z",
        "zakSprzed": "2020-04-10T22:23:45.678Z",
        "stPTU": [
            {
                "id": "A",
                "wart": 2300
            },
            {
                "id": "G",
                "wart": "ZW"
            }
        ],
        "sprzedPar": {
            "sumaBrutto": 49060,
            "sumaPod": 5060,
            "wartWgPTU": [
                {
                    "idStPTU": "A",
```

```
                    "netto": 22000,
                    "vat": 5060
                },
                {
                    "idStPTU": "G",
                    "netto": 20200,
                    "vat": 0
                }
            ]
        },
        "podatekNal": 5060,
        "sprzedBrutto": 49060,
        "waluta": "PLN",
        "liczbaPar": 4,
        "liczbaParAnul": 3,
        "wartParAnul": 111000000,
        "dokNiefisk": 1,
        "zakRap": "2020-04-10T23:23:45.678Z",
        "nrKasy": "001",
        "kasjer": "Kasjer",
        "podpis": {
            "RSA":
"21184e6e94b7c822223c90b3769567188c285c262d10be052c6820242368a5f655af1c77138930fe51873f2e2eea6
c6a7666f3f8cf9f1776dad23ce32afb687f6b5057bdf38ce3bb732ff27d95b1682c541b43410af8cad7262bc93dc74
66b09588311242b4c297251ae54afd8911607a482854a8bb326b68ae7c8d1295266488ee635a483e90157f8c943a3a
dd99329edbc2ca18d9954e976f32f4bda9d74eb99527f411436c8857d4b8e804e72b0c0e6a58e47a6975749b842187
4f095041cc5429d9d18b3f446f0c834964e2150c2f56b6de9e72f62cfa5f194aa5650a55b64f5f903d52b9435e8418
3860810835e5a266aef281b92ab8a257d9467f4c1ce",
            "SHA": "7d68d863163c76b46d26e543d44d0f7d373beef55d055f3ffb929484d9e374f4",
            "JPK": "00000000000000000000"
        }
    }
}
```


C.2.2c Ustrukturyzowana postać przykładowego dokumentu niefiskalnego:


```
{
    "wydrNiefisk": {
        "JPKID": 3,
        "pamiecChr": 1,
        "grafika": 1,
        "nrDok": 2,
        "zawart": [
            {
                "kodGraficzny": "kodGraficzny0",
                "kodKreskowy": "kodKreskowy0",
                "tekst": "tekst0"
            },
            {
                "tekst": [
                    "WYDRUK NIEFISKALNY",
                    "TEST"
                ],
                "kodKreskowy": [
                    "kodKreskowy1",
                    "kodKreskowy2"
                ],
                "kodGraficzny": [
                    "kodGraficzny1",
                    "kodGraficzny2"
                ]
            }
        ],
        "zak": "2020-04-10T03:23:45.678Z",
        "nrKasy": "001",
        "kasjer": "Kasjer",
        "podpis": {
            "RSA":
"282f2b77102bbb60717093d6ad9c2db648201be698baa316c03e7598446fc7915042e9d4a19d5a846ad5998c7467e
cedd1f545dc6619d6c0a17e55f9380d01e584dffa84971bc9e91f922e6f2f4fe243c1382b8fa067809451241992622
```

```
faa9e7b83feb4a3d6d8f742278c1e5174570a63b113495384a346ad6f1e0f5072d91c9227ea68abbbc9a902f0463a1
26fbb43ef1380dac8421cd8d45cb797ab75a7c3b08988709e64bc174d9aeead5e9ea1a44d01e0c3e0a7ecb97baec56
0f34f4a6ce34d27749d5b220384ce2d9add085e77a947be2b532c555ce0f5a92b9266cc262580ce7d56c528792d5a9
08b8a503b4188e3e77f3230cb53fc5e1cbba9c79fb1"
        }
    }
}
```


C.2.2d Ustrukturyzowana postać przykładowego paragonu fiskalnego anulowanego:


```
{
    "paragAnul": {
        "JPKID": 6,
        "pamiecChr": 1,
        "nrDok": 5,
        "pozycja": [
            {
                "towar": {
                    "brutto": 1000000,
                    "cena": 1000000,
                    "idStPTU": "G",
                    "ilosc": "1",
                    "nazwa": "Nazwa towaru",
                    "oper": false
                }
            }
        ],
        "stPTU": [
            {
                "id": "G",
                "wart": "ZW"
            }
        ],
        "podsum": {
            "sumaNetto": [
                {
                    "idStPTU": "G",
                    "brutto": 1000000,
                    "vat": 0
                }
            ],
            "sumaPod": 1000000,
            "sumaBrutto": 1000000,
            "waluta": "PLN"
        },
        "total": {
            "zaplZwrot": 1000000
        },
        "nrParag": 3,
        "nrKasy": "001",
        "zakSprzed": "2020-04-10T06:23:45.678Z",
        "kasjer": "Kasjer",
        "podpis": {
            "RSA":
"9e61a538a24334c0af624987d5967c11d89286f02bcd1c9123ff284c460e3dcf2ae7cca47c1a5079010b201d2a6ac
e3c1d619377c57501a3773e7faaa3ac3c2ea7eb26409b3ff852d715cf1c16cc1b490e7876bc23af51720174c729a2c
8aea7d4a58cf3d99b54582698764e58922af469d011cbc5100bb57bbbcf3f373bf629a33257eec641662c3f44cbc9d
39c7d7f885a1b8fcd6da954e918077f7ff3279e2f84ea9aa944ab9123dd10f711870a8d1d6856ecaa6a6df0a7bce17
03fd79376bec82cec37ea4ba48a64063ebcdf4d99f9e18c37d0777bd4437ca819d19b2a8b2f73cff076cb240ee0580
d90eaba0c7aad3dff10af58e64c03e51453caa1c8f3",
            "SHA": "eee0e3068482a34527630f4c73c05d0d3523899f5fa25d022b9415ff8057d3be",
            "JPK": "000000000000000000"
        }
    }
}
```


C.2.2e Ustrukturyzowana postać przykładowego paragonu fiskalnego anulowanego:


```
{
```

```
    "paragAnul": {
        "JPKID": 9,
        "pamiecChr": 1,
        "nrDok": 8,
        "pozycja": [
            {
                "towar": {
                    "brutto": 10000000,
                    "cena": 10000000,
                    "idStPTU": "G",
                    "ilosc": "1",
                    "nazwa": "Nazwa towaru",
                    "oper": false
                }
            }
        ],
        "stPTU": [
            {
                "id": "G",
                "wart": "ZW"
            }
        ],
        "podsum": {
            "sumaNetto": [
                {
                    "idStPTU": "G",
                    "brutto": 10000000,
                    "vat": 0
                }
            ],
            "sumaPod": 10000000,
            "sumaBrutto": 10000000,
            "waluta": "PLN"
        },
        "total": {
            "zaplZwrot": 10000000
        },
        "nrParag": 6,
        "nrKasy": "001",
        "zakSprzed": "2020-04-10T09:23:45.678Z",
        "kasjer": "Kasjer",
        "podpis": {
            "RSA":
"ab6c66f6f3cbc34dde1e8f3b3080bee64555ab5f3886bae21f4be9139a11f6c09bc8765f229bfd99bece7fb7dbb5c
f18ffc17e7cfbd56bc8b637d4a821e483d8b6c5cc947e356a543b5eba1020a499fe7506d49c5d3fbdb61dbd4281247
83fe0ee6532f57b7600d8266435eda9e5fead47c4d31b18961fe21ad824ccc6b20d51961a6221bcef4554322f3127c
9e488aaf6a54d049809648484066837 2b5cf6b22a73a26334249a74fb4c87568dbde4693dfeed4ec44f473dcf4921c
3da287f3e8b1085521a833b416c7a269fa6d03e1d23ea1fde9577c78ae60179b4303629674f1fdfbacaed55706a7b4
66957b93c083d1e3f4af231f503cdb694b9afb0ebf3",
            "SHA": "a64a913986f2a18d4db5ecbe02309fc96d19c683830622140a2d4310425f911c",
            "JPK": "0010000000000000006"
        }
    }
}
```


C.2.2f Ustrukturyzowana postać przykładowego paragonu fiskalnego anulowanego:


```
{
    "paragAnul": {
        "JPKID": 10,
        "pamiecChr": 1,
        "nrDok": 9,
        "pozycja": [
            {
                "towar": {
                    "brutto": 100000000,
                    "cena": 100000000,
                    "idStPTU": "G",
                    "ilosc": "1",
                    "nazwa": "Nazwa towaru",
```

```
                    "oper": false
                }
            }
        ],
        "stPTU": [
            {
                "id": "G",
                "wart": "ZW"
            }
        ],
        "podsum": {
            "sumaNetto": [
                {
                    "idStPTU": "G",
                    "brutto": 100000000,
                    "vat": 0
                }
            ],
            "sumaPod": 100000000,
            "sumaBrutto": 100000000,
            "waluta": "PLN"
        },
        "total": {
            "zaplZwrot": 100000000
        },
        "nrParag": 7,
        "nrKasy": "001",
        "zakSprzed": "2020-04-10T10:23:45.678Z",
        "kasjer": "Kasjer",
        "podpis": {
            "RSA":
"54ce7bad1079bc8a7a69908766aa6e420edf611442f28f28cfbd51c3c181ad54505ff81465ab6dbbd93fcaf0fb78b
83ef56304e83fb302bf0e07c2114b7a947ad20c012d204efe1cd53aaff0469830aabe01a8a5828c798872bd6dbb7d8
767ab832d892a40f81c07d7246e34f8716d5cd0fd206da3bbb89aae831010f3e2278a6ce76c9206b022e6a246a0b88
9cbe571c062bf214a3dd924168f4913bde545dba76f42875bb1c7060fd06ded94f9c9ab7e9f2d04f276b9ccfaebdbd
ac48cc92b5b4f629504daca05d887a1cd8e035e50d7b07af374609f3bd6080e4bed80330d62924987d440f0b06f7e9
9a3ec980df0e1951e073854e20173a937ec2f1ca93f",
            "SHA": "ac6450833bef0f47888dea1272d179e8a197c8b6968c16782eeaff4f2769430d",
            "JPK": "0010000000000000009"
        }
    }
}
```


C.2.3 Przykłady danych do podpisu dokumentów przesyłanych w zbiorach danych

C.2.3a Pełna postać przykładowych danych do podpisu raportu fiskalnego fiskalizacji:


```
6970000802WTE20010000092020-04-10T01:23:45.678Z9DD845A0C9C285DC2E13F3253352E1836DC603C0KW123
```


C.2.3b Pełna postać przykładowych danych do podpisu raportu fiskalnego dobowego:


```
6970000802WTE200100000949060506020 20-04-10T23:23:45.678Z
```


C.2.3c Pełna postać przykładowych danych do podpisu dokumentu niefiskalnego:


```
6970000802WTE200100000922020-04-10T03:23:45.678Z
```


C.2.3d Pełna postać przykładowych danych do podpisu paragonu anulowanego:


```
6970000802WTE2001000009510000002020-04-10T06:23:45.678Z
```

C.2.4 Przykładowe podpisy danych dokumentów przesyłanych w zbiorach danych

C.2.4a Pełna postać podpisu danych raportu fiskalnego fiskalizacji:

```
3019505879124143c92b60d5e57ebc08ba8fb7c9d2ce1bae02ba6b77a9c14b7794f7f8acbddff2c2e382fbb6820cd0
e0a87fa988f2c67f9b34ae0571cfc0b23b727b7912c9d30b567c56e710cbfa88f09937bbfd1c54065df893eafb7455
823716c292d548dc98dfc4ad29c81332450b84bea1a4bbf11e0c4dcc8d21f835476b87ff5a68be7d514fe15d3ebb76
c2559bfe93a8cdfd09bf9bab7b5df918225c2f46778f59fb9deef898eb4e932f405a1403d9e0e78772c25675f14edc
34d457f42aeb0a719a7a9638654bae7823641b1f95981b37fbd2cff3fda256e2e8f2e5aa8aca729e2d9a9b32893d66
64b223da5c1879afcec64fea8b11fe22a622de55bb
```

C.2.4b Pełna postać podpisu danych raportu fiskalnego dobowego:

```
21184e6e94b7c822223c90b3769567188c285c262d10be052c6820242368a5f655af1c77138930fe51873f2e2eea6c
6a7666f3f8cf9f1776dad23ce32afb687f6b5057bdf38ce3bb732ff27d95b1682c541b43410af8cad7262bc93dc746
6b09588311242b4c297251ae54afd8911607a482854a8bb326b68ae7c8d1295266488ee635a483e90157f8c943a3ad
d99329edbc2ca18d9954e976f32f4bda9d74eb99527f411436c8857d4b8e804e72b0c0e6a58e47a6975749b8421874
f095041cc5429d9d18b3f446f0c834964e2150c2f56b6de9e72f62cfa5f194aa5650a55b64f5f903d52b9435e84183
860810835e5a266aef281b92ab8a257d9467f4c1ce
```

C.2.4c Pełna postać podpisu danych dokumentu niefiskalnego:

```
282f2b77102bbb60717093d6ad9c2db648201be698baa316c03e7598446fc7915042e9d4a19d5a846ad5998c7467ec
edd1f545dc6619d6c0a17e55f9380d01e584dffa84971bc9e91f922e6f2f4fe243c1382b8fa067809451241992622f
aa9e7b83feb4a3d6d8f742278c1e5174570a63b113495384a346ad6f1e0f5072d91c9227ea68abbbc9a902f0463a12
6fbb43ef1380dac8421cd8d45cb797ab75a7c3b08988709e64bc174d9aeead5e9ea1a44d01e0c3e0a7ecb97baec560
f34f4a6ce34d27749d5b220384ce2d9add085e77a947be2b532c555ce0f5a92b9266cc262580ce7d56c528792d5a90
8b8a503b4188e3e77f3230cb53fc5e1cbba9c79fb1
```

C.2.4d Pełna postać podpisu danych paragonu anulowanego (pierwszego):

```
9e61a538a24334c0af624987d5967c11d89286f02bcd1c9123ff284c460e3dcf2ae7cca47c1a5079010b201d2a6ace
3c1d619377c57501a3773e7faaa3ac3c2ea7eb26409b3ff852d715cf1c16cc1b490e7876bc23af51720174c729a2c8
aea7d4a58cf3d99b54582698764e58922af469d011cbc5100bb57bbbcf3f373bf629a33257eec641662c3f44cbc9d3
9c7d7f885a1b8fcd6da954e918077f7ff3279e2f84ea9aa944ab9123dd10f711870a8d1d6856ecaa6a6df0a7bce170
3fd79376bec82cec37ea4ba48a64063ebcdf4d99f9e18c37d0777bd4437ca819d19b2a8b2f73cff076cb240ee0580d
90eaba0c7aad3dff10af58e64c03e51453caa1c8f3
```

C.2.4e Pełna postać podpisu danych paragonu anulowanego (drugiego):

```
ab6c66f6f3cbc34dde1e8f3b3080bee64555ab5f3886bae21f4be9139a11f6c09bc8765f229bfd99bece7fb7dbb5cf
18ffc17e7cfbd56bc8b637d4a821e483d8b6c5cc947e356a543b5eba1020a499fe7506d49c5d3fbdb61dbd42812478
3fe0ee6532f57b7600d8266435eda9e5fead47c4d31b18961fe21ad824ccc6b20d51961a6221bcef4554322f3127c9
e488aaf6a54d0498096484840668372b5cf6b22a73a26334249a74fb4c87568dbde4693dfeed4ec44f473dcf4921c3
da287f3e8b1085521a833b416c7a269fa6d03e1d23ea1fde9577c78ae60179b4303629674f1fdfbacaed55706a7b46
6957b93c083d1e3f4af231f503cdb694b9afb0ebf3
```

C.2.4f Pełna postać podpisu danych paragonu anulowanego (trzeciego):

```
54ce7bad1079bc8a7a69908766aa6e420edf611442f28f28cfbd51c3c181ad54505ff81465ab6dbbd93fcaf0fb78b8
3ef56304e83fb302bf0e07c2114b7a947ad20c012d204efe1cd53aaff0469830aabe01a8a5828c798872bd6dbb7d87
67ab832d892a40f81c07d7246e34f8716d5cd0fd206da3bbb89aae831010f3e2278a6ce76c9206b022e6a246a0b889
cbe571c062bf214a3dd924168f4913bde545dba76f42875bb1c7060fd06ded94f9c9ab7e9f2d04f276b9ccfaebdbda
c48cc92b5b4f629504daca05d887a1cd8e035e50d7b07af374609f3bd6080e4bed80330d62924987d440f0b06f7e99
a3ec980df0e1951e073854e20173a937ec2f1ca93f
```

C.2.5 Dane wejściowe służące do wyliczenia skrótu SHA2

C.2.5a Pełna postać danych wejściowych służących do wyliczenia skrótu SHA2 pierwszego paragonu anulowanego:

```
9e61a538a24334c0af624987d5967c11d89286f02bcd1c9123ff284c460e3dcf2ae7cca47c1a5079010b201d2a6ace
3c1d619377c57501a3773e7faaa3ac3c2ea7eb26409b3ff852d715cf1c16cc1b490e7876bc23af51720174c729a2c8
aea7d4a58cf3d99b54582698764e58922af469d011cbc5100bb57bbbcf3f373bf629a33257eec641662c3f44cbc9d3
9c7d7f885a1b8fcd6da954e918077f7ff3279e2f84ea9aa944ab9123dd10f711870a8d1d6856ecaa6a6df0a7bce170
3fd79376bec82cec37ea4ba48a64063ebcdf4d99f9e18c37d0777bd4437ca819d19b2a8b2f73cff076cb240ee0580d
90eaba0c7aad3dff10af58e64c03e51453caa1c8f3
```

C.2.5b Pełna postać danych wejściowych służących do wyliczenia skrótu SHA2 drugiego paragonu anulowanego:

```
eee0e3068482a34527630f4c73c05d0d3523899f5fa25d022b9415ff8057d3beab6c66f6f3cbc34dde1e8f3b3080be
e64555ab5f3886bae21f4be9139a11f6c09bc8765f229bfd99bece7fb7dbb5cf18ffc17e7cfbd56bc8b637d4a821e4
83d8b6c5cc947e356a543b5eba1020a499fe7506d49c5d3fbdb61dbd428124783fe0ee6532f57b7600d8266435eda9
e5fead47c4d31b18961fe21ad824ccc6b20d51961a6221bcef4554322f3127c9e488aaf6a54d049809648484066837
2b5cf6b22a73a26334249a74fb4c87568dbde4693dfeed4ec44f473dcf4921c3da287f3e8b1085521a833b416c7a26
9fa6d03e1d23ea1fde9577c78ae60179b4303629674f1fdfbacaed55706a7b466957b93c083d1e3f4af231f503cdb6
94b9afb0ebf3
```

C.2.5c Pełna postać danych wejściowych służących do wyliczenia skrótu SHA2 trzeciego paragonu anulowanego:

```
a64a913986f2a18d4db5ecbe02309fc96d19c683830622140a2d4310425f911c54ce7bad1079bc8a7a69908766aa6e
420edf611442f28f28cfbd51c3c181ad54505ff81465ab6dbbd93fcaf0fb78b83ef56304e83fb302bf0e07c2114b7a
947ad20c012d204efe1cd53aaff0469830aabe01a8a5828c798872bd6dbb7d8767ab832d892a40f81c07d7246e34f8
716d5cd0fd206da3bbb89aae831010f3e2278a6ce76c9206b022e6a246a0b889cbe571c062bf214a3dd924168f4913
bde545dba76f42875bb1c7060fd06ded94f9c9ab7e9f2d04f276b9ccfaebdbdac48cc92b5b4f629504daca05d887a1
cd8e035e50d7b07af374609f3bd6080e4bed80330d62924987d440f0b06f7e99a3ec980df0e1951e073854e20173a9
37ec2f1ca93f
```

C.3 Przykładowe dane procesu podpisywania dokumentów w postaci elektronicznej

C.3.1 Przykłady chronionego nagłówka dokumentów w postaci elektronicznej:

C.3.1a Pełna postać chronionego nagłówka paragonu fiskalnego (pierwszego):

{"eParagon.mf.gov.pl":"eyJ3ZXJzamEiOiJKUEtfS0FTQV9QQVJBR09OX3YxLTAiLCJKUEtJRCI6IjAwMTAwMDAwMDA
wMDAwMDAwNCIsImRhdGFKUEsiOiIyMDIwLTA0LTEwVDA0OjIzOjQ1LjY3OFoiLCJKUEtSRUYiOnsiU0hBMjU2IjoiMDAwM
DAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMCIsIkpQS0lEIjo
iMDAwMDAwMDAwMDAwMDAwMDAwIn19","alg":"RS256","jpkmetadata":"eyJjb3JyZWxhdGlvbklkIjoiVEZELldURT
IwMDEwMDAwMDkuMjAyMC0wNC0wM1QxMTo1MDowMC4zMjJaIiwiY29tcHJlc3Npb24iOiJOT05FIn0=","x5c":["MIIDKj
CCApOgAwIBAgIQ27uolIpDHKdAJjLSAHD4+zANBgkqhkiG9w0BAQsFADAUMRIwEAYDVQQDEwlNRiBlLUthc3kwHhcNMjAw
MzE2MTAzNTU5WhcNMjUwMzE2MTAzNTU4WjCBrjEjMCEGA1UECxMaRGVwYXJ0YW1lbnQgSW5mb3JtYXR5emFjamkxHjAcBg
NVBAoTFU1pbmlzdGVyc3R3byBGaW5hbnNvdzEZMBcGA1UEBRMQVkFUUEwtNjk3MDAwMDgwMjEWMBQGA1UEAxMNV1RFMjAw
MTAwMDAwOTERMA8GA1UEBxMIV2Fyc3phd2ExFDASBgNVBAgTC01hem93aWVja2llMQswCQYDVQQGEwJQTDCCASIwDQYJKo
ZIhvcNAQEBBQADggEPADCCAQoCggEBALtSH7AwSOT4qT863BAwbt2DvGqEgDNV\/g0dtWK81C5vK677mb9Y7U0PccRJG4h
t7B+kmRvfsO92YgnjmpQEqAJj4GyCicGXaI+6f6xeUQknwvpAHvpmPGvZjlsAmHyScLdGqOXzQgrxV\/WE64jJgendcucs
Gu6AZHRCW7rxGMAxGA2ySgEpNZBQq8hphl7sAjj0PHZCJwU5PP1nsNzddSOEJndJYHNbbrom6ZFLbju2QMk\/gWpFACgYV
9hoHiOo7BCSiZ3fPC4tpmhxOPqmdZDYwInSU0MgaYP3p803z2f16g1kg2Tldt4GroubKiffW4RumFwuIPZZe8DKD834PQ8
CAwEAAaNeMFwwEwYDVR0lBAwwCgYIKwYBBQUHAwIwRQYDVR0BBD4wPIAQxg+n+j1jAU1f23nuS65XPaEWMBQxEjAQBgNVB
AMTCU1GIGUtS2FzeYIQs8LVeZ9uP5lAlnvXe8bYejANBgkqhkiG9w0BAQsFAAOBgQBZfk\/KxEy\/3zIfP0r4Nt5Dg5LbJ
737kRfIZRhu3PHmMthAac2kTLtaaaWC+iL70nm8t\/J9kRD9Uyk83vLmLbPGVEbcOlY+5Oo5XYetubSdLFnLm4kiFUDh5N
P4AKzQdTpCp4jbAOWRFJCbrZZbV6M0XytAE\/mlrTrml9K313MxRw=="]}

C.3.1b Pełna postać chronionego nagłówka paragonu fiskalnego (drugiego):

{"eParagon.mf.gov.pl":"eyJ3ZXJzamEiOiJKUEtfS0FTQV9QQVJBR09OX3YxLTAiLCJKUEtJRCI6IjAwMTAwMDAwMDA
wMDAwMDAwNSIsImRhdGFKUEsiOiIyMDIwLTA0LTEwVDA1OjIzOjQ1LjY3OFoiLCJKUEtSRUYiOnsiU0hBMjU2IjoiRjg4R
TZFNUFEOTU2MTk1MDcyRkM0Mzc5NTRBQjNCQTA1RjBGM0ZGNjc3RjZBMDEyOUNCOUVGRkM4MzUzOEJBMCIsIkpQS0lEIjo
iMDAxMDAwMDAwMDAwMDAwMDA0In19","alg":"RS256","jpkmetadata":"eyJjb3JyZWxhdGlvbklkIjoiVEZELldURT
IwMDEwMDAwMDkuMjAyMC0wNC0wM1QxMTo1MDowMC4zMjJaIiwiY29tcHJlc3Npb24iOiJERUZMQVRFIn0=","x5c":["MI
IDKjCCApOgAwIBAgIQ27uolIpDHKdAJjLSAHD4+zANBgkqhkiG9w0BAQsFADAUMRIwEAYDVQQDEwlNRiBlLUthc3kwHhcN
MjAwMzE2MTAzNTU5WhcNMjUwMzE2MTAzNTU4WjCBrjEjMCEGA1UECxMaRGVwYXJ0YW1lbnQgSW5mb3JtYXR5emFjamkxHj
AcBgNVBAoTFU1pbmlzdGVyc3R3byBGaW5hbnNvdzEZMBcGA1UEBRMQVkFUUEwtNjk3MDAwMDgwMjEWMBQGA1UEAxMNV1RF
MjAwMTAwMDAwOTERMA8GA1UEBxMIV2Fyc3phd2ExFDASBgNVBAgTC01hem93aWVja2llMQswCQYDVQQGEwJQTDCCASIwDQ
YJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALtSH7AwSOT4qT863BAwbt2DvGqEgDNV\/g0dtWK81C5vK677mb9Y7U0PccR
JG4ht7B+kmRvfsO92YgnjmpQEqAJj4GyCicGXaI+6f6xeUQknwvpAHvpmPGvZjlsAmHyScLdGqOXzQgrxV\/WE64jJgend
cucsGu6AZHRCW7rxGMAxGA2ySgEpNZBQq8hphl7sAjj0PHZCJwU5PP1nsNzddSOEJndJYHNbbrom6ZFLbju2QMk\/gWpFA
CgYV9hoHiOo7BCSiZ3fPC4tpmhxOPqmdZDYwInSU0MgaYP3p803z2f16g1kg2Tldt4GroubKiffW4RumFwuIPZZe8DKD83
4PQ8CAwEAAaNeMFwwEwYDVR0lBAwwCgYIKwYBBQUHAwIwRQYDVR0BBD4wPIAQxg+n+j1jAU1f23nuS65XPaEWMBQxEjAQB
gNVBAMTCU1GIGUtS2FzeYIQs8LVeZ9uP5lAlnvXe8bYejANBgkqhkiG9w0BAQsFAAOBgQBZfk\/KxEy\/3zIfP0r4Nt5Dg
5LbJ737kRfIZRhu3PHmMthAac2kTLtaaaWC+iL70nm8t\/J9kRD9Uyk83vLmLbPGVEbcOlY+5Oo5XYetubSdLFnLm4kiFU
Dh5NP4AKzQdTpCp4jbAOWRFJCbrZZbV6M0XytAE\/mlrTrml9K313MxRw=="]}

C.3.1c Pełna postać chronionego nagłówka paragonu fiskalnego (trzeciego):

{"eParagon.mf.gov.pl":"eyJ3ZXJzamEiOiJKUEtfS0FTQV9QQVJBR09OX3YxLTAiLCJKUEtJRCI6IjAwMTAwMDAwMDA
wMDAwMDAwNyIsImRhdGFKUEsiOiIyMDIwLTA0LTEwVDA3OjIzOjQ1LjY3OFoiLCJKUEtSRUYiOnsiU0hBMjU2IjoiNzc2O
UMzODlCQjMzQzdGMzRCMDZEMUNCNkMwREExM0Y5QUQzMDU4NUJGRTQ3QjdEQjA4NUEyQTI2ODkwRTEwMSIsIkpQS0lEIjo
iMDAxMDAwMDAwMDAwMDAwMDA1In19","alg":"RS256","jpkmetadata":"eyJjb21wcmVzc2lvbiI6IkRFRkxBVEUifQ
==","x5c":["MIIDKjCCApOgAwIBAgIQ27uolIpDHKdAJjLSAHD4+zANBgkqhkiG9w0BAQsFADAUMRIwEAYDVQQDEwlNRi
BlLUthc3kwHhcNMjAwMzE2MTAzNTU5WhcNMjUwMzE2MTAzNTU4WjCBrjEjMCEGA1UECxMaRGVwYXJ0YW1lbnQgSW5mb3Jt
YXR5emFjamkxHjAcBgNVBAoTFU1pbmlzdGVyc3R3byBGaW5hbnNvdzEZMBcGA1UEBRMQVkFUUEwtNjk3MDAwMDgwMjEWMB
QGA1UEAxMNV1RFMjAwMTAwMDAwOTERMA8GA1UEBxMIV2Fyc3phd2ExFDASBgNVBAgTC01hem93aWVja2llMQswCQYDVQQG
EwJQTDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALtSH7AwSOT4qT863BAwbt2DvGqEgDNV\/g0dtWK81C5vK
677mb9Y7U0PccRJG4ht7B+kmRvfsO92YgnjmpQEqAJj4GyCicGXaI+6f6xeUQknwvpAHvpmPGvZjlsAmHyScLdGqOXzQgr
xV\/WE64jJgendcucsGu6AZHRCW7rxGMAxGA2ySgEpNZBQq8hphl7sAjj0PHZCJwU5PP1nsNzddSOEJndJYHNbbrom6ZFL
bju2QMk\/gWpFACgYV9hoHiOo7BCSiZ3fPC4tpmhxOPqmdZDYwInSU0MgaYP3p803z2f16g1kg2Tldt4GroubKiffW4Rum
FwuIPZZe8DKD834PQ8CAwEAAaNeMFwwEwYDVR0lBAwwCgYIKwYBBQUHAwIwRQYDVR0BBD4wPIAQxg+n+j1jAU1f23nuS65
XPaEWMBQxEjAQBgNVBAMTCU1GIGUtS2FzeYIQs8LVeZ9uP5lAlnvXe8bYejANBgkqhkiG9w0BAQsFAAOBgQBZfk\/KxEy\
/3zIfP0r4Nt5Dg5LbJ737kRfIZRhu3PHmMthAac2kTLtaaaWC+iL70nm8t\/J9kRD9Uyk83vLmLbPGVEbcOlY+5Oo5XYet
ubSdLFnLm4kiFUDh5NP4AKzQdTpCp4jbAOWRFJCbrZZbV6M0XytAE\/mlrTrml9K313MxRw=="]}

C.3.1d Pełna postać chronionego nagłówka paragonu fiskalnego (czwartego):


```
{"eParagon.mf.gov.pl":"eyJ3ZXJzamEiOiJKUEtfS0FTQV9QQVJBR09OX3YxLTAiLCJKUEtJRCI6IjAwMTAwMDAwMDA
wMDAwMDAwOCIsImRhdGFKUEsiOiIyMDIwLTA0LTEwVDA4OjIzOjQ1LjY3OFoiLCJKUEtSRUYiOnsiU0hBMjU2IjoiQkJGN
DNEQThGMUJCMzFBRTZGMzE0OTkwNTczMkM1MEFEN0E4OEJDNkEyQ0UyQTkzNjBCNDVDQkMxQ0RDRjBGMSIsIkpQS0lEIjo
iMDAxMDAwMDAwMDAwMDAwMDA3In19","alg":"RS256","x5c":["MIIDKjCCApOgAwIBAgIQ27uolIpDHKdAJjLSAHD4+
zANBgkqhkiG9w0BAQsFADAUMRIwEAYDVQQDEwlNRiBlLUthc3kwHhcNMjAwMzE2MTAzNTU5WhcNMjUwMzE2MTAzNTU4WjC
BrjEjMCEGA1UECxMaRGVwYXJ0YW1lbnQgSW5mb3JtYXR5emFjamkxHjAcBgNVBAoTFU1pbmlzdGVyc3R3byBGaW5hbnNvd
zEZMBcGA1UEBRMQVkFUUEwtNjk3MDAwMDgwMjEWMBQGA1UEAxMNV1RFMjAwMTAwMDAwOTERMA8GA1UEBxMIV2Fyc3phd2E
xFDASBgNVBAgTC01hem93aWVja2llMQswCQYDVQQGEwJQTDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALtSH
7AwSOT4qT863BAwbt2DvGqEgDNV\/g0dtWK81C5vK677mb9Y7U0PccRJG4ht7B+kmRvfsO92YgnjmpQEqAJj4GyCicGXaI
+6f6xeUQknwvpAHvpmPGvZjlsAmHyScLdGqOXzQgrxV\/WE64jJgendcucsGu6AZHRCW7rxGMAxGA2ySgEpNZBQq8hphl7
sAjj0PHZCJwU5PP1nsNzddSOEJndJYHNbbrom6ZFLbju2QMk\/gWpFACgYV9hoHiOo7BCSiZ3fPC4tpmhxOPqmdZDYwInS
U0MgaYP3p803z2f16g1kg2Tldt4GroubKiffW4RumFwuIPZZe8DKD834PQ8CAwEAAaNeMFwwEwYDVR0lBAwwCgYIKwYBBQ
UHAwIwRQYDVR0BBD4wPIAQxg+n+j1jAU1f23nuS65XPaEWMBQxEjAQBgNVBAMTCU1GIGUtS2FzeYIQs8LVeZ9uP5lAlnvX
e8bYejANBgkqhkiG9w0BAQsFAAOBgQBZfk\/KxEy\/3zIfP0r4Nt5Dg5LbJ737kRfIZRhu3PHmMthAac2kTLtaaaWC+iL7
0nm8t\/J9kRD9Uyk83vLmLbPGVEbcOlY+5Oo5XYetubSdLFnLm4kiFUDh5NP4AKzQdTpCp4jbAOWRFJCbrZZbV6M0XytAE
\/mlrTrml9K313MxRw=="]}
```


C.3.2 Przykłady chronionego nagłówka dokumentów w postaci elektronicznej w Base64URL:

C.3.2a Pełna postać chronionego nagłówka paragonu fiskalnego (pierwszego) zakodowana w Base64URL:


```
eyJlUGFyYWdvbi5tZi5nb3YucGwiOiJleUozWlhKemFtRWlPaUpLVUV0ZlMwRlRRVjlRUVZKQlIwOU9YM1l4TFRBaUxDSk
tVRXRKUkNJNklqQXdNVEF3TURBd01EQXdNREF3TURBd05DSXNJbVJoZEdGS1VFc2lPaUl5TURJd0xUQTBMVEV3VkRBME9q
SXpPalExTGpZM09Gb2lMQ0pLVUV0U1JVWWlPbnNpVTBoQk1qVTJJam9pTURBd01EQXdNREF3TURBd01EQXdNREF3TURBd0
1EQXdNREF3TURBd01EQXdNREF3TURBd01EQXdNREF3TURBd01EQXdNREF3TUNJc0lrcFFTMGxFSWpv
aU1EQXdNREF3TURBd01EQXdNREF3TURBd0luMTkiLCJhbGciOiJSUzI1NiIsImpwa2lldGFkYXRhIjoiZXlKamIzSnlaV3
hoZEdsdmJrbGtJam9pVkVaRUxsZFVSVEl3TURFd01EQXdNRGt1TWpBeU1DMHdOQzB3TTFReE1UbzFNRG93TUM0ek1qSmFJ
aXdpWTI5dGNISmxjM05wYjI0aU9pSk9UMDVGSW4wPSIsIng1YyI6WyJNSUlES2pDQ0FwT2dBd0lCQWdJUTI3dW9sSXBESE
tkQUpqTFNBSEQ0K3pBTkJna3Foa2lHOXcwQkFRc0ZBREFVTVJJd0VBWURWUVFERXdsTlJpQmxMVXRoYzNrd0hoY05NakF3
TXpFMk1UQXpOVFU1V2hjTk1qVXdNekUyTVRBek5UVTRXakNCcmpFak1DRUdBMVVFQ3hNYVJHVndZWEowWVcxbGJuUWdTVz
VtYjNKdFlYUjVlbUZqYW1reEhqQWNCZ05WQkFvVEZVMXBibWx6ZEdWeWMzUjNieUJHYVc1aGJuTnZkekVaTUJjR0ExVUVC
Uk1RVmtGVVVFd3ROamszTURBd01EZ3dNakVXTUJRR0ExVUVBeE1OVjFSRk1qQXdNVEF3TURBd09URVJNQThHQTFVRUJ4TU
lWMkZ5YzNwaGQyRXhGREFTQmdOVkJBZ1RDMDFoZW05M2FXVmphMmxsTVFzd0NRWURWUVFHRXdKUVREQ0NBU0l3RFFZSktv
WklodmNOQVFFQkJRQURnZ0VQQURDQ0FRb0NnZ0VCQUx0U0g3QXdTT1Q0cVQ4NjNCQXdidDJEdkdxRWdETlZcL2cwZHRXSz
gxQzV2SzY3N21iOVk3VTBQY2NSSkc0aHQ3QitrbVJ2ZnNPOTJZZ25qbXBRRXFBSmo0R3lDaWNHWGFJKzZmNnhlVVFrbnd2
cEFIdnBtUEd2Wmpsc0FtSHlTY0xkR3FPWHpRZ3J4VlwvV0U2NGpKZ2VuZGN1Y3NHdTZBWkhSQ1c3cnhHTUF4R0EyeVNnRX
BOWkJRcThocGhsN3NBamowUEhaQ0p3VTVQUDFuc056ZGRTT0VKbmRKWUhOYmJyb202WkZMYmp1MlFNa1wvZ1dwRkFDZ1lW
OWhvSGlPbzdCQ1NpWjNmUEM0dHBtaHhPUHFtZFpEWXdJblNVME1nYVlQM3A4MDN6MmYxNmcxa2cyVGxkdDRHcm91YktpZm
ZXNFJ1bUZ3dUlQWlplOERLRDgzNFBROENBd0VBQWFOZU1Gd3dFd1lEVlIwbEJBd3dDZ1lJS3dZQkJRVUhBd0l3UlFZRFZS
MEJCRDR3UElBUXhnK24rajFqQVUxZjIzbnVTNjVYUGFFV01CUXhFakFRQmdOVkJBTVRDVTFHSUdVdFMyRnplWUlRczhMVm
VaOXVQNWxBbG52WGU4YlllakFOQmdrcWhraUc5dzBCQVFzRkFBT0JnUUJaZmtcL0t4RXlcLzN6SWZQMHI0TnQ1RGc1TGJK
NzM3a1JmSVpSaHUzUEhtTXRoQWFjMmtUTHRhYWFXQytpTDcwbm04dFwvSjlrUkQ5VXlrODN2TG1MYlBHVkViY09sWSs1T2
81WFlldHViU2RMRm5MbTRraUZVRGg1TlA0QUt6UWRUcENwNGpiQU9XUkZKQ2JyWlpiVjZNMFh5dEFFXC9tbHJUcm1sOUsz
MTNNeFJ3PT0iXX0
```


C.3.2b Pełna postać chronionego nagłówka paragonu fiskalnego (drugiego) zakodowana w Base64URL:


```
eyJlUGFyYWdvbi5tZi5nb3YucGwiOiJleUozWlhKemFtRWlPaUpLVUV0ZlMwRlRRVjlRUVZKQlIwOU9YM1l4TFRBaUxDSk
tVRXRKUkNJNklqQXdNVEF3TURBd01EQXdNREF3TURBd05TSXNJbVJoZEdGS1VFc2lPaUl5TURJd0xUQTBMVEV3VkRBMU9q
SXpPalExTGpZM09Gb2lMQ0pLVUV0U1JVWWlPbnNpVTBoQk1qVTJJam9pUmpnNFJUWkZOVUZFT1RVMk1UazFNRGN5UmtNME
16YzVOVFJCUWpOQ1FUQTFSakJHTTBaR05qYzNSalpCTURFeU9VTkNPVVZHUmtNNE16VXpPRUpCTUNJc0lrcFFTMGxFSWpv
aU1EQXhNREF3TURBd01EQXdNREF3TURBMEluMTkiLCJhbGciOiJSUzI1NiIsImpwa2lldGFkYXRhIjoiZXlKamIzSnlaV3
hoZEdsdmJrbGtJam9pVkVaRUxsZFVSVEl3TURFd01EQXdNRGt1TWpBeU1DMHdOQzB3TTFReE1UbzFNRG93TUM0ek1qSmFJ
aXdpWTI5dGNISmxjM05wYjI0aU9pSkVSVVpNUVZSRkluMD0iLCJ4NWMiOlsiTUlJREtqQ0NBcE9nQXdJQkFnSVEyN3VvbE
lwREhLZEFKakxTQUhENCt6QU5CZ2txaGtpRzl3MEJBUXNGQURBVU1SSXdFQVlEVlFREV3bE5aUJsTFV0aGMza3dIaGNO
TWpBd016RTJNVEF6TlRVNVdoY05qVXpNVXpPVFU0V2pDQnJqRWpNQ0VHQTFVRUN4TWFSR1Z3WVhKMFlXMWxibl
FnU1c1bWIzSnRZWFI1ZW1GamFta3hIakFjQmdOVkJBb1RGVTFwYm1semRHVnljM1IzYnlCR2FXNWhibk52ZHpFWk1CY0dB
MVVFQlJNUVZrRlVVRXd0TmprM01EQXdNRGd3TWpFV01CUUdBMVVFQXhNTlYxUkZNakF3TVRBd01EQXdPVEVSTUE4R0ExVU
VCeE1JVjJGeWMzcGhkMkV4RkRBU0JnTlZCQWdUQzAxaGVtOTNhV1ZqYTJsbE1Rc3dDUVlEVlFRR0V3SlFURENDQVNJd0RR
WUpLb1pJaHZjTkFRUJCUUFEZ2dFUEFEQ0NBUW9DZ2dFQkFMdFNIN0F3U09UNHFUODYzQkF3YnQyRHZHcUVnRE5WXC9nMG
R0V0s4MUM1dks2NzdtYjlZN1UwUGNjUkpHNGh0N0Ira21SdmZzTzkyWWduam1wUUVxQUpqNEd5Q2ljR1hhSSs2ZjZ4ZVVR
a253dnBBSHZwbVBHdlpqbHNBbUh5U2NMZEdxT1h6UWdyeFZcL1dFNjRqSmdlbmRjdWNzR3U2QVpIUkNXN3J4R01BeEdBMn
```

lTZ0VwTlpCUXE4aHBobDdzQWpqMFBIWkNKd1U1UFAxbnNOemRkU09FSm5kSllITmJicm9tNlpGTGJqdTJRTWtcL2dXcEZB
Q2dZVjlob0hpT283QkNTaVozZlBDNHRwbWh4T1BxbWRaRFl3SW5TVTBNZ2FZUDNwODAzejJmMTZnMWtnMlRsZHQ0R3JvdW
JLaWZmVzRSdW1Gd3VJUFpaZThES0Q4MzRQUThDQXdFQUFhTmVNRnd3RXdZRFZSMGxCQXd3Q2dZSUt3WUJCUVVIQXdJd1JR
WURWUjBCQkQ0d1BJQVF4ZytuK2oxakFVMWYyM251UzY1WFBhRVdNQlF4RWpBUUJnTlZCQU1UQ1UxR0lHVXRTMkZ6ZVlJUX
M4TFZlWjl1UDVsQWxudlhlOGJZZWpBTkJna3Foa2lHOXcwQkFRc0ZBQU9CZ1FCWmZrXC9LeEV5XC8zeklmUDByNE50NURn
NUxiSjczN2tSZklaUmh1M1BIbU10aEFhYzJrVEx0YWFhV0MraUw3MG5tOHRcL0o5a1JEOVV5azgzdkxtTGJQR1ZFYmNPbF
krNU9vNVhZZXR1YlNkTEZuTG00a2lGVURoNU5QNEFLelFkVHBDcDRqYkFPV1JGSkNiclpaYlY2TTBYeXRBRVwvbWxyVHJt
bDlLMzEzTXhSdz09Il19

C.3.2c Pełna postać chronionego nagłówka paragonu fiskalnego (trzeciego) zakodowana w Base64URL:

eyJlUGFyYWdvbi5tZi5nb3YucGwiOiJleUozWlhKemFtRWlPaUpLVUV0ZlMwRlRRVjlRUVZKQlIwOU9YM1l4TFRBaUxDSk
tVRXRKUkNJNklqQXdNVEF3TURBd01EQXdNREF3TURBd055SXNJbVJoZEdGS1VFc2lPaUl5TURJd0xUQTBMVEV3VkRBM09q
SXpPalExTGpZM09Gb2lMQ0pLVUV0U1JVWWlPbnNpVTBoQk1qVTJJam9pTnpjMk9VTXpPRGxDUWpNelF6ZEdNelJDTURaRU
1VTkNOa013UkVFeE0wWTVRVVF6TURVNE5VSkdSVFEzUWpkRVFqQTROVUV5UVRJMk9Ea3dSVEV3TVNJc0lrcFFTMGxFSWpv
aU1EQXhNREF3TURBd01EQXdNREF3TURBMUluMTkiLCJhbGciOiJSUzI1NiIsImpwa2lldGFkYXRhIjoiZXlKamIyMXdjbV
Z6YzJsdmJpSTZJa1JGUmt4Q1lZFVWlmUT09IiwieDVjIjpbIk1JSURLakNDQXBPZ0F3SUJBZ0lRMjd1b2xJcERIS2RBSmpM
U0FIRDQrekFOQmdrcWhraUc5dzBCQVFzRkFEQVVNUkl3RUFZRFZRUURFd2xOUmlCbExVdGhjM2t3SGhjTk1qQXdNekUyTV
RBek5UVTVXaGNOTWpVd016RTJNVEF6TlRVNFdqQ0JyakVqTUNFR0ExVUVDeE1hUkdWd1lYSjBZVzFsYm5RZ1NXNW1iM0p0
WVhSNWVtRmphbWt4SGpBY0JnTlZCQW9URlUxcGJtbHpkR1Z5YzNSM2J5QkdhVzVoYm5OdmR6RVpNQmNHQTFVRUJSTVFWa0
ZVVUV3dE5qazNNREF3TURnd01qRVdNQlFHQTFVRUF4TU5WMVJGTWpBd01UQXdNREF3T1RFUk1BOEdBMVVFQnhNSVYyRnlj
M3BoZDJFeEZEQVNCZ05WQkFnVEMwMWhlbTkzYVdWamEybGxNUXN3Q1FZRFZRUUdFd0pRVERDQ0FTSXdEUVlKS29aSWh2Y0
5BUUVCQlFBRGdnRVBBRENDQVFvQ2dnRUJBTHRTSDdBd1NPVDRxVDg2M0JBd2J0MkR2R3FFZ0ROVlwvZzBkdFdLODFDNXZL
Njc3bWI5WTdVMFBjY1JKRzRodDdCK2ttUnZmc085MllnbmptcFFFcUFKajRHeUNpY0dYYUkrNmY2eGVVUWtud3ZwQUh2cG
1QR3ZaamxzQW1IeVNjTGRHcU9YelFncnhWXC9XRTY0akpnZW5kY3Vjc0d1NkFaSFJDVzdyeEdNQXhHQTJ5U2dFcE5aQlFx
OGhwaGw3c0FqajBQSFpDSndVNVBQMW5zTnpkZFNPRUpuZEpZSE5iYnJvbTZaRkxianUyUU1rXC9nV3BGQUNnWVY5aG9IaU
9vN0JDU2laM2ZQQzR0cG1oeE9QcW1kWkRZd0luU1UwTWdhWVAzcDgwM3oyZjE2ZzFrZzJUbGR0NEdyb3ViS2lmZlc0UnVt
Rnd1SVBaWmU4REtEODM0UFE4Q0F3RUFBYU5lTUZ3d0V3WURWUjBsQkF3d0NnWUlLd1lCQlFVSEF3SXdSUVlEVlIwQkJENH
dQSUFReGcrbitqMWpBVTFmMjNudVM2NVhQYUVXTUJReEVqQVFCZ05WQkFNVENVMUdJR1V0UzJGemVZSVFzOExWZVo5dVA1
bEFsbnZYZThiWWVqQU5CZ2txaGtpRzl3MEJBUXNGQUFPQmdRQlpma1wvS3hFeVwvM3pJZlAwcjROdDVEZzVMYko3MzdrUm
ZJWlJodTNQSG1NdGhBYWMya1RMdGFhYVdDK2lMNzBubTh0XC9KOWtSRDlVeWs4M3ZMbUxiUEdWRWJjT2xZKzVPbzVYWWV0
dWJTZExGbkxtNGtpRlVEaDVOUDRBS3pRZFRwQ3A0amJBT1dSRkpDYnJaWmJWNk0wWHl0QUVcL21sclRybWw5SzMxM014Un
c9PSJdfQ

C.3.2d Pełna postać chronionego nagłówka paragonu fiskalnego (czwartego) zakodowana w Base64URL:

eyJlUGFyYWdvbi5tZi5nb3YucGwiOiJleUozWlhKemFtRWlPaUpLVUV0ZlMwRlRRVjlRUVZKQlIwOU9YM1l4TFRBaUxDSk
tVRXRKUkNJNklqQXdNVEF3TURBd01EQXdNREF3TURBd09DSXNJbVJoZEdGS1VFc2lPaUl5TURJd0xUQTBMVEV3VkRBNE9q
SXpPalExTGpZM09Gb2lMQ0pLVUV0U1JVWWlPbnNpVTBoQk1qVTJJam9pUWtKR05ETkVRVGhHTVVKQ016RkJSVFpHTXpFME
9Ua3dOVGN6TWtNMU1FRkVOMEU0T0VKRE5rRXlRMFV5UVRrek5qQkNORFZEUWtNeFEwUkRSakJHTVNJc0lrcFFTMGxFSWpv
aU1EQXhNREF3TURBd01EQXdNREF3TURBM0luMTkiLCJhbGciOiJSUzI1NiIsIng1YyI6WyJNSUlES2pDQ0FwT2dBd0lCQW
dJUTI3dW9sSXBESEtkQUpqTFNBSEQ0K3pBTkJna3Foa2lHOXcwQkFRc0ZBREFVTVJJd0VBWURWUVFERXdsTlJpQmxMVXRo
YzNrd0hoY05NakF3TXpFMk1UQXpOVFU1V2hjTk1qVXdNekUyTVRBek5UVTRXakNCcmpFak1DRUdBMVVFQ3hNYVJHVndZWE
owWVcxbGJuUWdTVzVtYjNKdFlYUjVlbUZqYW1reEhqQWNCZ05WQkFvVEZVMXBibWx6ZEdWeWMzUjNieUJHYVc1aGJuTnZk
ekVaTUJjR0ExVUVCUk1RVmtGVVVFd3ROamszTURBd01EZ3dNakVXTUJRR0ExVUVBeE1OVjFSRk1qQXdNVEF3TURBd09URV
JNQThHQTFVRUJ4TUlWMkZ5YzNwaGQyRXhGREFTQmdOVkJBZ1RDMDFoZW05M2FXVmphMmxsTVFzd0NRWURWUVFHRXdKUVRE
Q0NBU0l3RFFZSktvWklodmNOQVFFQkJRQURnZ0VQQURDQ0FRb0NnZ0VCQUx0U0g3QXdTT1Q0cVQ4NjNCQXdidDJEdkdxRW
dETlZcL2cwZHRXSzgxQzV2SzY3N21iOVk3VTBQY2NSSkc0aHQ3QitrbVJ2ZnNPOTJZZ25qbXBRRXFBSmo0R3lDaWNHWGFJ
KzZmNnhlVVFrbnd2cEFIdnBtUEd2Wmpsc0FtSHlTY0xkR3FPWHpRZ3J4VlwvV0U2NGpKZ2VuZGN1Y3NHdTZBWkhSQ1c3cn
hHTUF4R0EyeVNnRXBOWkJRcThocGhsN3NBamowUEhaQ0p3VTVQUDFuc056ZGRTT0VKbmRKWUhOYmJyb202WkZMYmp1MlFN
a1wvZ1dwRkFDZ1lWOWhvSGlPbzdCQ1NpWjNmUEM0dHBtaHhPUHFtZFpEWXdJblNVME1nYVlQM3A4MDN6MmYxNmcxa2cyVG
xkdDRHcm91YktpZmZXNFJ1bUZ3dUlQWlplOERLRDgzNFBROENBd0VBQWFOZU1Gd3dFd1lEVlIwbEJBd3dDZ1lJS3dZQkJR
VUhBd0l3UlFZRFZSMEJCRDR3UElBUXhnK24rajFqQVUxZjIzbnVTNjVYUGFFV01CUXhFakFRQmdOVkJBTVRDVTFHSUdVdF
MyRnplWUlRczhMVmVaOXVQNWxBbG52WGU4YlllakFOQmdrcWhraUc5dzBCQVFzRkFBT0JnUUJaZmtcL0t4RXlcLzN6SWZQ
MHI0TnQ1RGc1TGJKNzM3a1JmSVpSaHUzUEhtTXRoQWFjMmtUTHRhYWFXQytpTDcwbm04dFwvSjlrUkQ5VXlrODN2TG1MYl
BHVkViY09sWSs1T281WFlldHViU2RMRm5MbTRraUZVRGg1TlA0QUt6UWRUcENwNGpiQU9XUkZKQ2JyWlpiVjZNMFh5dEFF
XC9tbHJUcm1sOUszMTNNeFJ3PT0iXX0

C.3.3 Przykłady ustrukturyzowanych danych dokumentów w postaci elektronicznej:

C.3.3a Przykładowa postać ustrukturyzowanych danych paragonu fiskalnego (pierwszego):


```
{
    "dokument": {
        "naglowek": {
            "wersja": "JPK_KASA_PARAGON_v1-0",
            "dataJPK": "2020-04-10T04:23:45.678Z"
        },
        "podmiot1": {
            "nazwaPod": "Nazwa podmiotu",
            "nrFabr": "WTE2001000009",
            "NIP": "6970000802",
            "adresPod": {
                "ulica": "Ulica",
                "miejsc": "Miejscowosc",
                "nrLok": "NrLok",
                "poczta": "Poczta",
                "nrDomu": "NrDomu",
                "kodPoczt": "00-000"
            },
            "nrUnik": "WTE2001000009",
            "nrEwid": "2020/000001612"
        },
        "paragon": {
            "JPKID": 4,
            "pamiecChr": 1,
            "nrDok": 3,
            "pozycja": [
                {
                    "towar": {
                        "brutto": 1230,
                        "cena": 1230,
                        "idStPTU": "A",
                        "ilosc": "1",
                        "nazwa": "Nazwa towaru 1",
                        "oper": false
                    }
                },
                {
                    "towar": {
                        "brutto": 1000,
                        "cena": 1000,
                        "idStPTU": "G",
                        "ilosc": "1",
                        "nazwa": "Nazwa towaru 2",
                        "oper": false
                    }
                }
            ],
            "stPTU": [
                {
                    "id": "A",
                    "wart": 2300
                },
                {
                    "id": "G",
                    "wart": "ZW"
                }
            ],
            "podsum": {
                "sumaNetto": [
                    {
                        "idStPTU": "A",
                        "brutto": 1230,
                        "vat": 230
                    },
                    {
```

```
                    "idStPTU": "G",
                    "brutto": 1000,
                    "vat": 0
                }
            ],
            "sumaPod": 230,
            "sumaBrutto": 2230,
            "waluta": "PLN"
        },
        "total": {
            "zaplZwrot": 2230
        },
        "nrParag": 1,
        "nrKasy": "001",
        "zakSprzed": "2020-04-10T04:23:45.678Z",
        "kasjer": "Kasjer"
    }
  }
}
```

C.3.3b Przykładowa postać ustrukturyzowanych danych paragonu fiskalnego (drugiego):

```
{
    "dokument": {
        "naglowek": {
            "wersja": "JPK_KASA_PARAGON_v1-0",
            "dataJPK": "2020-04-10T05:23:45.678Z"
        },
        "podmiot1": {
            "nazwaPod": "Nazwa podmiotu",
            "nrFabr": "WTE2001000009",
            "NIP": "6970000802",
            "adresPod": {
                "ulica": "Ulica",
                "miejsc": "Miejscowosc",
                "nrLok": "NrLok",
                "poczta": "Poczta",
                "nrDomu": "NrDomu",
                "kodPoczt": "00-000"
            },
            "nrUnik": "WTE2001000009",
            "nrEwid": "2020/000001612"
        },
        "paragon": {
            "JPKID": 5,
            "pamiecChr": 1,
            "nrDok": 4,
            "pozycja": [
                {
                    "towar": {
                        "brutto": 1230,
                        "cena": 1230,
                        "idStPTU": "A",
                        "ilosc": "1",
                        "nazwa": "Nazwa towaru 1",
                        "oper": false
                    }
                },
                {
                    "towar": {
                        "brutto": 1000,
                        "cena": 1000,
                        "idStPTU": "G",
                        "ilosc": "1",
                        "nazwa": "Nazwa towaru 2",
                        "oper": false
                    }
                }
            ],
            "stPTU": [
```

```
                {
                    "id": "A",
                    "wart": 2300
                },
                {
                    "id": "G",
                    "wart": "ZW"
                }
            ],
            "podsum": {
                "sumaNetto": [
                    {
                        "idStPTU": "A",
                        "brutto": 1230,
                        "vat": 230
                    },
                    {
                        "idStPTU": "G",
                        "brutto": 1000,
                        "vat": 0
                    }
                ],
                "sumaPod": 230,
                "sumaBrutto": 2230,
                "waluta": "PLN"
            },
            "total": {
                "zaplZwrot": 2230
            },
            "nrParag": 2,
            "nrKasy": "001",
            "zakSprzed": "2020-04-10T05:23:45.678Z",
            "kasjer": "Kasjer"
        }
    }
}
```

C.3.3c Przykładowa postać ustrukturyzowanych danych paragonu fiskalnego (trzeciego):

```
{
    "dokument": {
        "naglowek": {
            "wersja": "JPK_KASA_PARAGON_v1-0",
            "dataJPK": "2020-04-10T07:23:45.678Z"
        },
        "podmiot1": {
            "nazwaPod": "Nazwa podmiotu",
            "nrFabr": "WTE2001000009",
            "NIP": "6970000802",
            "adresPod": {
                "ulica": "Ulica",
                "miejsc": "Miejscowosc",
                "nrLok": "NrLok",
                "poczta": "Poczta",
                "nrDomu": "NrDomu",
                "kodPoczt": "00-000"
            },
            "nrUnik": "WTE2001000009",
            "nrEwid": "2020/000001612"
        },
        "paragon": {
            "JPKID": 7,
            "pamiecChr": 1,
            "nrDok": 6,
            "pozycja": [
                {
                    "towar": {
                        "brutto": 12300,
                        "cena": 12300,
                        "idStPTU": "A",
```

```
                    "ilosc": "1",
                    "nazwa": "Nazwa towaru 1",
                    "oper": false
                }
            },
            {
                "towar": {
                    "brutto": 10000,
                    "cena": 10000,
                    "idStPTU": "G",
                    "ilosc": "1",
                    "nazwa": "Nazwa towaru 2",
                    "oper": false
                }
            }
        ],
        "stPTU": [
            {
                "id": "A",
                "wart": 2300
            },
            {
                "id": "G",
                "wart": "ZW"
            }
        ],
        "podsum": {
            "sumaNetto": [
                {
                    "idStPTU": "A",
                    "brutto": 12300,
                    "vat": 2300
                },
                {
                    "idStPTU": "G",
                    "brutto": 10000,
                    "vat": 0
                }
            ],
            "sumaPod": 2300,
            "sumaBrutto": 22300,
            "waluta": "PLN"
        },
        "total": {
            "zaplZwrot": 22300
        },
        "nrParag": 4,
        "nrKasy": "001",
        "zakSprzed": "2020-04-10T07:23:45.678Z",
        "kasjer": "Kasjer"
    }
  }
}
```

C.3.3d Przykładowa postać ustrukturyzowanych danych paragonu fiskalnego (czwartego):

```
{
    "dokument": {
        "naglowek": {
            "wersja": "JPK_KASA_PARAGON_v1-0",
            "dataJPK": "2020-04-10T08:23:45.678Z"
        },
        "podmiot1": {
            "nazwaPod": "Nazwa podmiotu",
            "nrFabr": "WTE2001000009",
            "NIP": "6970000802",
            "adresPod": {
                "ulica": "Ulica",
                "miejsc": "Miejscowosc",
                "nrLok": "NrLok",
```

```
                "poczta": "Poczta",
                "nrDomu": "NrDomu",
                "kodPoczt": "00-000"
            },
            "nrUnik": "WTE2001000009",
            "nrEwid": "2020/000001612"
        },
        "paragon": {
            "JPKID": 8,
            "pamiecChr": 1,
            "nrDok": 7,
            "pozycja": [
                {
                    "towar": {
                        "brutto": 12300,
                        "cena": 12300,
                        "idStPTU": "A",
                        "ilosc": "1",
                        "nazwa": "Nazwa towaru 1",
                        "oper": false
                    }
                },
                {
                    "towar": {
                        "brutto": 10000,
                        "cena": 10000,
                        "idStPTU": "G",
                        "ilosc": "1",
                        "nazwa": "Nazwa towaru 2",
                        "oper": false
                    }
                }
            ],
            "stPTU": [
                {
                    "id": "A",
                    "wart": 2300
                },
                {
                    "id": "G",
                    "wart": "ZW"
                }
            ],
            "podsum": {
                "sumaNetto": [
                    {
                        "idStPTU": "A",
                        "brutto": 12300,
                        "vat": 2300
                    },
                    {
                        "idStPTU": "G",
                        "brutto": 10000,
                        "vat": 0
                    }
                ],
                "sumaPod": 2300,
                "sumaBrutto": 22300,
                "waluta": "PLN"
            },
            "total": {
                "zaplZwrot": 22300
            },
            "nrParag": 5,
            "nrKasy": "001",
            "zakSprzed": "2020-04-10T08:23:45.678Z",
            "kasjer": "Kasjer"
        }
    }
}
```

C.3.4 Przykłady nieskompresowanych danych dokumentów w postaci elektronicznej:

C.3.4a Przykładowa postać nieskompresowanych danych paragonu fiskalnego (pierwszego):


```
{"dokument":{"naglowek":{"wersja":"JPK_KASA_PARAGON_v1-0","dataJPK":"2020-04-
10T04:23:45.678Z"},"paragon":{"pamiecChr":1,"total":{"zaplZwrot":2230},"zakSprzed":"2020-04-
10T04:23:45.678Z","JPKID":4,"nrParag":1,"kasjer":"Kasjer","stPTU":[{"id":"A","wart":2300},{"id
":"G","wart":"ZW"}],"podsum":{"waluta":"PLN","sumaNetto":[{"brutto":1230,"vat":230,"idStPTU":"
A"},{"brutto":1000,"vat":0,"idStPTU":"G"}],"sumaBrutto":2230,"sumaPod":230},"nrDok":3,"pozycja
":[{"towar":{"brutto":1230,"ilosc":"1","oper":false,"cena":1230,"nazwa":"Nazwa towaru
1","idStPTU":"A"}},{"towar":{"brutto":1000,"ilosc":"1","oper":false,"cena":1000,"nazwa":"Nazwa
towaru 2","idStPTU":"G"}}],"nrKasy":"001"},"podmiot1":{"nazwaPod":"Nazwa
podmiotu","nrFabr":"WTE2001000009","NIP":"6970000802","adresPod":{"ulica":"Ulica","miejsc":"Mi
ejscowosc","nrLok":"NrLok","poczta":"Poczta","nrDomu":"NrDomu","kodPoczt":"00-
000"},"nrUnik":"WTE2001000009","nrEwid":"2020/000001612"}}}
```


C.3.4b Przykładowa postać nieskompresowanych danych paragonu fiskalnego (drugiego):


```
{"dokument":{"naglowek":{"wersja":"JPK_KASA_PARAGON_v1-0","dataJPK":"2020-04-
10T05:23:45.678Z"},"paragon":{"pamiecChr":1,"total":{"zaplZwrot":2230},"zakSprzed":"2020-04-
10T05:23:45.678Z","JPKID":5,"nrParag":2,"kasjer":"Kasjer","stPTU":[{"id":"A","wart":2300},{"id
":"G","wart":"ZW"}],"podsum":{"waluta":"PLN","sumaNetto":[{"brutto":1230,"vat":230,"idStPTU":"
A"},{"brutto":1000,"vat":0,"idStPTU":"G"}],"sumaBrutto":2230,"sumaPod":230},"nrDok":4,"pozycja
":[{"towar":{"brutto":1230,"ilosc":"1","oper":false,"cena":1230,"nazwa":"Nazwa towaru
1","idStPTU":"A"}},{"towar":{"brutto":1000,"ilosc":"1","oper":false,"cena":1000,"nazwa":"Nazwa
towaru 2","idStPTU":"G"}}],"nrKasy":"001"},"podmiot1":{"nazwaPod":"Nazwa
podmiotu","nrFabr":"WTE2001000009","NIP":"6970000802","adresPod":{"ulica":"Ulica","miejsc":"Mi
ejscowosc","nrLok":"NrLok","poczta":"Poczta","nrDomu":"NrDomu","kodPoczt":"00-
000"},"nrUnik":"WTE2001000009","nrEwid":"2020/000001612"}}}
```


C.3.4c Przykładowa postać nieskompresowanych danych paragonu fiskalnego (trzeciego):


```
{"dokument":{"naglowek":{"wersja":"JPK_KASA_PARAGON_v1-0","dataJPK":"2020-04-
10T07:23:45.678Z"},"paragon":{"pamiecChr":1,"total":{"zaplZwrot":22300},"zakSprzed":"2020-04-
10T07:23:45.678Z","JPKID":7,"nrParag":4,"kasjer":"Kasjer","stPTU":[{"id":"A","wart":2300},{"id
":"G","wart":"ZW"}],"podsum":{"waluta":"PLN","sumaNetto":[{"brutto":12300,"vat":2300,"idStPTU"
:"A"},{"brutto":10000,"vat":0,"idStPTU":"G"}],"sumaBrutto":22300,"sumaPod":2300},"nrDok":6,"po
zycja":[{"towar":{"brutto":12300,"ilosc":"1","oper":false,"cena":12300,"nazwa":"Nazwa towaru
1","idStPTU":"A"}},{"towar":{"brutto":10000,"ilosc":"1","oper":false,"cena":10000,"nazwa":"Naz
wa towaru 2","idStPTU":"G"}}],"nrKasy":"001"},"podmiot1":{"nazwaPod":"Nazwa
podmiotu","nrFabr":"WTE2001000009","NIP":"6970000802","adresPod":{"ulica":"Ulica","miejsc":"Mi
ejscowosc","nrLok":"NrLok","poczta":"Poczta","nrDomu":"NrDomu","kodPoczt":"00-
000"},"nrUnik":"WTE2001000009","nrEwid":"2020/000001612"}}}
```


C.3.4d Przykładowa postać nieskompresowanych danych paragonu fiskalnego (czwartego):


```
{"dokument":{"naglowek":{"wersja":"JPK_KASA_PARAGON_v1-0","dataJPK":"2020-04-
10T08:23:45.678Z"},"paragon":{"pamiecChr":1,"total":{"zaplZwrot":22300},"zakSprzed":"2020-04-
10T08:23:45.678Z","JPKID":8,"nrParag":5,"kasjer":"Kasjer","stPTU":[{"id":"A","wart":2300},{"id
":"G","wart":"ZW"}],"podsum":{"waluta":"PLN","sumaNetto":[{"brutto":12300,"vat":2300,"idStPTU"
:"A"},{"brutto":10000,"vat":0,"idStPTU":"G"}],"sumaBrutto":22300,"sumaPod":2300},"nrDok":7,"po
zycja":[{"towar":{"brutto":12300,"ilosc":"1","oper":false,"cena":12300,"nazwa":"Nazwa towaru
1","idStPTU":"A"}},{"towar":{"brutto":10000,"ilosc":"1","oper":false,"cena":10000,"nazwa":"Naz
wa towaru 2","idStPTU":"G"}}],"nrKasy":"001"},"podmiot1":{"nazwaPod":"Nazwa
podmiotu","nrFabr":"WTE2001000009","NIP":"6970000802","adresPod":{"ulica":"Ulica","miejsc":"Mi
ejscowosc","nrLok":"NrLok","poczta":"Poczta","nrDomu":"NrDomu","kodPoczt":"00-
000"},"nrUnik":"WTE2001000009","nrEwid":"2020/000001612"}}}
```

C.3.5 Przykłady danych dokumentów w postaci elektronicznej zakodowane w Base64URL:

C.3.5a Przykładowa postać danych paragonu fiskalnego (pierwszego) w Base64URL:

eyJkb2t1bWVudCI6eyJuYWdsb3dlayI6eyJ3ZXJzamEiOiJKUEtfS0FTQV9QQVJBR09OX3YxLTAiLCJkYXRhSlBLIjoiMj
AyMC0wNC0xMFQwNDoyMzo0NS42NzhaIn0sInBhcmFnb24iOnsicGFtaWVjQ2hyIjoxLCJ0b3RhbCI6eyJ6YXBsWndyb3Qi
OjIyMzB9LCJ6YWtTcHJ6ZWQiOiIyMDIwLTA0LTEwVDA0OjIzOjQ1LjY3OFoiLCJKUEtJRCI6NCwibnJQYXJhZyI6MSwia2
FzamVyIjoiS2FzamVyIiwic3RQVFUiOlt7ImlkIjoiQSIsIndhcnQiOjIzMDB9LHsiaWQiOiJHIiwid2FydCI6IlpXIn1d
LCJwb2RzdW0iOnsid2FsdXRhIjoiUExOIiwic3VtYU5ldHRvIjpbeyJicnV0dG8iOjEyMzAsInZhdCI6MjMwLCJpZFN0UF
RVIjoiQSJ9LHsiYnJ1dHRvIjoxMDAwLCJ2YXQiOjAsImlkU3RQVFUiOiJHIn1dLCJzdW1hQnJ1dHRvIjoyMjMwLCJzdW1h
UG9kIjoyMzB9LCJuckRvayI6MywicG96eWNqYSI6W3sidG93YXIiOnsiYnJ1dHRvIjoxMjMwLCJpbG9zYyI6IjEiLCJvcG
VyIjpmYWxzZSwiY2VuYSI6MTIzMCwibmF6d2EiOiJOYXp3YSB0b3dhcnUgMSIsImlkU3RQVFUiOiJBIn19LHsidG93YXIi
OnsiYnJ1dHRvIjoxMDAwLCJpbG9zYyI6IjEiLCJvcGVyIjpmYWxzZSwiY2VuYSI6MTAwMCwibmF6d2EiOiJOYXp3YSB0b3
dhcnUgMiIsImlkU3RQVFUiOiJHIn19XSwibnJLYXN5IjoiMDAxIn0sInBvZG1pb3QxIjp7Im5hendhUG9kIjoiTmF6d2Eg
cG9kbWlvdHUiLCJuckZhYnIiOiJXVEUyMDAxMDAwMDA5IiwiTklQIjoiNjk3MDAwMDgwMiIsImFkcmVzUG9kIjp7InVsaW
NhIjoiVWxpY2EiLCJtaWVqc2MiOiJNaWVqc2Nvd29zYyIsIm5yTG9rIjoiTnJMb2siLCJwb2N6dGEiOiJQb2N6dGEiLCJu
ckRvbXUiOiJOckRvbXUiLCJrb2RQb2N6dCI6IjAwLTAwMCJ9LCJuclVuaWsiOiJXVEUyMDAxMDAwMDA5IiwibnJFd2lkIj
oiMjAyMC8wMDAwMDE2MTIifX19

C.3.5b Przykładowa postać danych paragonu fiskalnego (drugiego) w Base64URL:

hVLbbtNAEP2Vap43sHYubf1maIlKirFIokpBKNraS3F8WWu9rlVH-Xdmxkml QAV-
2fFczjlz2UNq8rbUlYNgD5V6Kkync7I7bZudggA-x4vtIlyG2zj8Fs6_RttnbyRBQKqcwhhm-
NKXIzkZeXIlp4E_DibTd7PLqw0cBNTKqidTEWKtykwnH39ZCDwBzjhVkLtXdbHprEEFvj-
WWNOrfFnbXqf_whYk7O4GgqmAysZEgwACctXsNFLAYjAENC5erSH4voeMEEN0dcoS3Vgi3dE9f3XD5gEOP1C6SZu25Fmoo
nU0i_g-
IsC2VJF2zjDoo23Z9BBOwLMagAWiLgdiZCSW1zwpT3lnWXMmJewPx0yfccgTm5RRD9TrjcEFTUhf_5LQilCEM6idpJ6ryQ
rTJIjtoWpT01h-qqLRAhJdqVNSpfqOmovovWCk9oIqzjqgFv5m4V7-x8JJb7L48McEaASVxdW94L-UHp-QScvMOG-
4UKzmaRyBjsEWqO6TeqTNP6xufayV9F1jILqL0Tu7viTHlSRSlVrdMM4e2iJLSNmaXwF4pTvu5wsbpqPuCP6eBg8RvyQr6
YejGIxhNWXLKWzgMZqUo9zMCNmBN7iusvwNnZW97bLT0b9ntzfzfJzK4Tc

C.3.5c Przykładowa postać danych paragonu fiskalnego (trzeciego) w Base64URL:

hVJtb5tADP4rlT9ftoNmScs3tnZRl46hJVGlTFPkwq0jvBw6jqIS5b_PPmikdtX2CeOznxfbB0h13paqshAcoMKHQncq57
hTptkjBPAlXu6W4SrcxeH3cPEt2j16EwkCUrRIb1ThS19O5HTiybWcB_55MP3wbja_2MJRQI0GH3TFiDWWmUo-
_TYQeAKstlhwuse62HZGkwLfP5eSmnrMV7XpVfovcMHKbq4gmAuoTMw8EEwF5NjsFXHAcggENDZebyD4cYCMEUNKdWiYz9
GN6cUpDds7OP4k7Tpt2tINA4vW8jDi24gB2xIjZa12oPemdaHHcAIecUQWhLsaqImTeU6VUp4qX5QtHC_DfxxL_QGJU7FO
nyWT4StNa5qxyP4p4UWREqvJAOt9JSkrdJMQvEfadc3D-
YVFowQkqsJTVYV9xx4j_p45rPaMW17YYB9_8wyG_sczVL3J48OrOfAgKkM7fKJ_KT13TDotM2294Vap241kBBofW-C-
z3jPJ3C3vvapl3nlJT1ENzFlZ5dzTlxIJsXUqMbhHKAtsoSVbdxXAN3r3hn66gLdsT2Gv-XhQ-S-LCvph-
sYgmE9ZetKXEBXqVP36sxMiB3cFjdVlr-hszLXXfZ8_e9d2pt5Pk3l-Ac

C.3.5d Przykładowa postać danych paragonu fiskalnego (czwartego) w Base64URL:

eyJkb2t1bWVudCI6eyJuYWdsb3dlayI6eyJ3ZXJzamEiOiJKUEtfS0FTQV9QQVJBR09OX3YxLTAiLCJkYXRhSlBLIjoiMj
AyMC0wNC0xMFQwODoyMzo0NS42NzhaIn0sInBhcmFnb24iOnsicGFtaWVjQ2hyIjoxLCJ0b3RhbCI6eyJ6YXBsWndyb3Qi
OjIyMzAwfSwiemFrU3ByemVkIjoiMjAyMC0wNC0xMFQwODoyMzo0NS42NzhaIiwiSlBLSUQiOjgsIm5yUGFyYWciOjUsIm
thc2plciI6Ikthc2plciIsInN0UFRVIjpbeyJpZCI6IkEiLCJ3YXJ0IjoyMzAwfSx7ImlkIjoiRyIsIndhcnQiOiJaVyJ9
XSwicG9kc3VtIjp7IndhbHV0YSI6IlBMTiIsInN1bWFOZXR0byI6W3siYnJ1dHRvIjoxMjMwMCwidmF0IjoyMzAwLCJpZF
N0UFRVIjoiQSJ9LHsiYnJ1dHRvIjoxMDAwMCwidmF0IjowLCJpZFN0UFRVIjoiRyJ9XSwic3VtYUJydXR0byI6MjIzMDAs
InN1bWFQb2QiOjIzMDB9LCJuckRvayI6NywicG96eWNqYSI6W3sidG93YXIiOnsiYnJ1dHRvIjoxMjMwMCwiaWxvc2MiOi
IxIiwib3BlciI6ZmFsc2UsImNlbmEiOjEyMzAwLCJuYXp3YSI6Ik5hendhIHRvd2FydSAxIiwiaWRTdFBUVSI6IkEifX0s
eyJ0b3dhciI6eyJicnV0dG8iOjEwMDAwLCJpbG9zYyI6IjEiLCJvcGVyIjpmYWxzZSwiY2VuYSI6MTAwMDAsIm5hendhIj
oiTmF6d2EgdG93YXJ1IDIiLCJpZFN0UFRVIjoiRyJ9fV0sImp5yS2FzeSI6IjAwMSJ9LCJwb2RtaW90MSI6eyJuYXp3YVBv
ZCI6Ik5hendhIHBvZG1pb3R1IiwibnJGYWJyIjoiV1RFMjAwMTAwMDAwOSIsIk5JUCI6IjY5NzAwMDA4MDIiLCJhZHJlc1
BvZCI6eyJ1bGljYSI6IlVsaWNhIiwibWllanNjIjoiTWllanNjb3dvc2MiLCJuckxvayI6Ik5yTG9rIiwicG9jenRhIjoi
UG9jenRhIiwibnJEb211IjoiTnJEb211Iiwia29kUG9jenQiOiIwMC0wMDAifSwibnJVbmlrIjoiV1RFMjAwMTAwMDAwOS
IsIm5yRXdpZCI6IjIwMjAvMDAwMDAxNjEyIn19fQ

C.3.6 Przykładowe obiekty JWS dokumentów w postaci elektronicznej:

C.3.6a Pełna postać obiektu JWS paragonu fiskalnego w postaci elektronicznej (pierwszego):

eyJlUGFyYWdvbi5tZi5nb3YucGwiOiJleUozWlhKemFtRWlPaUpLVUV0ZlMwRlRRVjlRUVZKQlIwOU9YM1l4TFRBaUxDSktVRXRKUkNJNklqQXdN
VEF3TURBd01EQXdNREF3TURBd05DSXNJbVJoZEdGS1VFc2lPaUl5TURJd0xUQTBMVEV3VkRBME9qSXpPalExTGpZM09Gb2lMQ0pLVUV0U1JV
WWlPbnNpVTBoQk1qVTJJam9pTURBd01EQXdNREF3TURBd01EQXdNREF3TURBd01EQXdNREF3TURBd01EQXdNREF3TURBd01EQXdNREF3T
URBd01EQXdNREF3TURBd01EQXdNREF3TUNJc0lrcFFTMGxFSWpvaU1EQXdNREF3TURBd01EQXdNREF3TURBd0luMTkiLCJhbGciOiJSUzI1NiIs
Impwa21ldGFkYXRhIjoiZXlKamIzSnlaV3hoZEdsdmJrbGtJam9pVkVaRUxsZFVSVEl3TURFd01EQXdNRGt1TWpBeU1DMHdOQzB3TTFReE1UbzF
NRG93TUM0ek1qSmFJaXdpWTI5dGNISmxjM05wYjI0aU9pSk9UMDVGSW4wPSIsIng1YyI6WyJNSUlES2pDQ0FwT2dBd0lCQWdJUTI3dW9sSXB
ESEtkQUpqTFNBSEQ0K3pBTkJna3Foa2lHOXcwQkFRc0ZBREFVTVJJd0VBWURWUVFERXdsTlJpQmxMVXRoYzNrd0hoY05NakF3TXpFMk1UQXp
OVFU1V2hjTk1qVXdNekUyTVRBek5UVTRXakNCcmpFak1DRUdBMVVFQ3hNYVJHVndZWEowWVcxbGJuUWdTVzVtYjNKdFlYUjVlbUZqYW1re
EhqQWNCZ05WQkFvVEZVMXBibWx6ZEdWeWMzUjNieUJHYVc1aGJuTnZkekVaTUJjR0ExVUVCUk1RVmtGVVVFd3ROamszTURBd01EZ3dNak
VXTUJRR0ExVUVBeE1OVjFSRk1qQXdNVEF3TURBd09URVJNQThHQTFVRUJ4TUlWMkZ5YzNwaGQyRXhGREFTQmdOVkJBZ1RDMDFoZW05M
2FXVmphMmxsTVFzd0NRWURWUVFHRXdKUVREQ0NBU0l3RFFZSktvWklodmNOQVFFQkJRQURnZ0VQQURDQ0FRb0NnZ0VCQUx0U0g3QXd
TT1Q0cVQ4NjNCQXdidDJEdkdxRWdETlZcL2cwZHRXSzgxQzV2SzY3N21iOVk3VTBQY2NSSkc0aHQ3QitrbVJ2ZnNPOTJZZ25qbXBRRXFBSmo0R3l
DaWNHWGFJKzZmNnhlVVFrbnd2cEFIdnBtUEd2Wmpsc0FtSHlTY0xkR3FPWHpRZ3J4VlwvV0U2NGpKZ2VuZGN1Y3NHdTZBWkhSQ1c3cnhHTU
F4R0EyeVNnRXBOWkJRcThocGhsN3NBamowUEhaQ0p3VTVQUDFuc056ZGRTT0VKbmRKWUhOYmJyb202WkZMYmp1MlFNa1wvZ1dwRkFD
Z1lWOWhvSGlPbzdCQ1NpWjNmUEM0dHBtaHhPUHFtZFpEWXdJblNVME1nYVlQM3A4MDN6MmYxNmcxa2cyVGxkdDRHcm91YktpZmZXNFJ
1bUZ3dUlQWlplOERLRDgzNFBROENBd0VBQWFOZU1Gd3dFd1lEVlIwbEJBd3dDZ1lJS3dZQkJRVUhBd0l3UlFZRFZSMEJCRDR3UElBUXhnK24raj
FqQVUxZjIzbnVTNjVYUGFFV01CUXhFakFRQmdOVkJBTVRDVTFHSUdVdFMyRnplWUlRczhMVmVaOXVQNWxBbG52WGU4YlllakFOQmdrcWh
raUc5dzBCQVFzRkFBT0JnUUJaZmtcL0t4RXlcLzN6SWZQMHI0TnQ1RGc1TGJKNzM3a1JmSVpSaHUzUEhtTXRoQWFjMmtUTHRhYWFXQytpTDc
wbm04dFwvSjlrUkQ5VXlrODN2TG1MYlBHVkViY09sWSs1T281WFlldHViU2RMRm5MbTRraUZVRGg1TlA0QUt6UWRUcENwNGpiQU9XUkZKQ
2JyWlpiVjZNMFh5dEFFXC9tbHJUcm1sOUszMTNNeFJ3PT0iXX0.eyJkb2t1bWVudCI6eyJuYWdsb3dlayI6eyJ3ZXJzamEiOiJKUEtfS0FTQV9QQVJB
R09OX3YxLTAiLCJkYXRhSlBLIjoiMjAyMC0wNC0xMFQwNDoyMzo0NS42NzhaIn0sInBhcmFnb24iOnsicGFtaWVjQ2hyIjoxLCJ0b3RhbCI6eyJ6YX
BsWndyb3QiOjIyMzB9LCJ6YWtTcHJ6ZWQiOiIyMDIwLTA0LTEwVDA0OjIzOjQ1LjY3OFoiLCJKUEtJRCI6NCwibnJQYXJhZyI6MSwia2FzamVyIjoiS2
FzamVyIiwic3RQVFUiOlt7ImlkIjoiQSIsIndhcnQiOjIzMDB9LHsiaWQiOiJHIiwid2FydCI6IlpXIn1dLCJwb2RzdW0iOnsid2FsdXRhIjoiUExOIiwic3VtY
U5ldHRvIjpbeyJicnV0dG8iOjEyMzAsInZhdCI6MjMwLCJpZFN0UFRVIjoiQSJ9LHsiYnJ1dHRvIjoxMDAwLCJ2YXQiOjAsImlkU3RQVFUiOiJHIn1dLCJ
zdW1hQnJ1dHRvIjoyMjMwLCJzdW1hUG9kIjoyMzB9LCJuckRvayI6MywicG96eWNqYSI6W3sidG93YXIiOnsiYnJ1dHRvIjoxMjMwLCJpbG9zYyI6I
jEiLCJvcGVyIjpmYWxzZSwiY2VuYSI6MTIzMCwibmF6d2EiOiJOYXp3YSB0b3dhcnUgMSIsImlkU3RQVFUiOiJBIn19LHsidG93YXIiOnsiYnJ1dHRvIjo
xMDAwLCJpbG9zYyI6IjEiLCJvcGVyIjpmYWxzZSwiY2VuYSI6MTAwMCwibmF6d2EiOiJOYXp3YSB0b3dhcnUgMiIsImlkU3RQVFUiOiJHIn19XSwib
nJLYXN5IjoiMDAxIn0sInBvZG1pb3QxIjp7Im5hendhUG9kIjoiTmF6d2EgcG9kbWlvdHUiLCJuckZhYnIiOiJXVEUyMDAxMDAwMDA5IiwiTklQIjoiNj
k3MDAwMDgwMiIsImFkcmVzUG9kIjp7InVsaWNhIjoiVWxpY2EiLCJtaWVqc2MiOiJNaWVqc2Nvd29zYyIsIm5yTG9rIjoiTnJMb2siLCJwb2N6dGE
iOiJQb2N6dGEiLCJuckRvbXUiOiJOckRvbXUiLCJrb2RQb2N6dCI6IjAwLTAwMCJ9LCJuclVuaWsiOiJXVEUyMDAxMDAwMDA5IiwibnJFd2lkIjoiMjA
yMC8wMDAwMDE2MTIifX19.RmYbrkaNGEeKsxTym7dq1qin4JExmssGqcdzvgdfS9gUkz8O2KSQLNxfYhcUzT5Tp4cxhqtKgwNMCia69f6Fowbq
XExhHo6l1HjfNJJNZfkxDNAgp2HWTnPhKMcuy0oGlL8PS_NpudZsOZ17U4WcIswgdimb9IKpaoZupE8GFLNYN6NVQpWQVDi3Pjzi2_I7EJzz04uG
H39_mTmmfE9s-EWCFokg71mTWcxHwlEFBCJ-i6hCtZnuaRpOkVKywapt-
nUKwKbP3QESYF_EPOoLZBYZlbpJddTqRfUXtsTs3pe5rOsjRUlOSwmFToRQBrs8a8YgsyaXwz4zui_fOrXxsg

C.3.6b Pełna postać obiektu JWS paragonu fiskalnego w postaci elektronicznej (drugiego):

eyJlUGFyYWdvbi5tZi5nb3YucGwiOiJleUozWlhKemFtRWlPaUpLVUV0ZlMwRlRRVjlRUVZKQlIwOU9YM1l4TFRBaUxDSktVRXRKUkNJNklqQXdN
VEF3TURBd01EQXdNREF3TURBd05TSXNJbVJoZEdGS1VFc2lPaUl5TURJd0xUQTBMVEV3VkRBMU9qSXpPalExTGpZM09Gb2lMQ0pLVUV0U1JV
WWlPbnNpVTBoQk1qVTJJam9pUmpnNFJUWkZOVUZFT1RVMk1UazFNRGN5UmtNME16YzVOVFJCUWpOQ1FUQTFSakJHTTBaR05qYzNSalpC
TURFeU9VTkNPVVZHUmtNNE16VXpPRUpCTUNJc0lrcFFTMGxFSWpvaU1EQXhNREF3TURBd01EQXdNREF3TURBMEluMTkiLCJhbGciOiJSUzI1
NiIsImpwa21ldGFkYXRhIjoiZXlKamIzSnlaV3hoZEdsdmJrbGtJam9pVkVaRUxsZFVSVEl3TURFd01EQXdNRGt1TWpBeU1DMHdOQzB3TTFReE1U
bzFNRG93TUM0ek1qSmFJaXdpWTI5dGNISmxjM05wYjI0aU9pSkVSVVpNUVZSRkluMD0iLCJ4NWMiOlsiTUlJREtqQ0NBcE9nQXdJQkFnSVEyN3
VvbElwREhLZEFKakxTQUhENCt6QU5CZ2txaGtpRzl3MEJBUXNGQURBVU1SSXdFQVlEVlFRREV3bE5SaUJsTFV0aGMza3dIaGNOTWpBd016RTJNVEF6
NVEF6TlRVNVdoY05NalV3TXpFMk1UQXpOVFU0V2pDQnJqRWpNQ0VHQTFVRUN4TWFSR1Z3WVhKMFlXMWxiblFnU1c1bWIzSnRZWFI1ZW1
GamFta3hIakFjQmdOVkJBb1RGVTFwYm1semRHVnljM1IzYnlCR2FXNWhibk52ZHpFWk1CY0dBMVVFQlJNUVZrRlVVRXd0TmprM01EQXdNRG
d3TWpFV01CUUdBMVVFQXhNTlYxUkZNakF3TVRBd01EQXdPVEVSTUE4R0ExVUVCeE1JVjJGeWMzcGhkMkV4RkRBU0JnTlZCQWdUQzAxaGVt
OTNhV1ZqYTJsbE1Rc3dDUVlEVlFRR0V3SlFURENDQVNJd0RRWUpLb1pJaHZjTkFRRUJCUUFEZ2dFUEFEQ0NBUW9DZ2dFQkFMdFNIN0F3U09U
NHFUODYzQkF3YnQyRHZHcUVnRE5WXC9nMGR0V0s4MUM1dks2NzdtYjlZN1UwUGNjUkpHNGh0N0Ira21SdmZzTzkyWWduam1wUUVxQUp
qNEd5Q2ljR1hhSSs2ZjZ4ZVVRa253dnBBSHdwbVBHdlpqbHNBbUh5U2NMZEdxT1h6UWdyeFZcL1dFNjRqSmdlbmRjdWNzR3U2QVpIUkNXN3J
4R01BeEdBMnlTZ0VwTlZCQnlTZllIanlpcUXE4aHBobDdzQWpqMFBIWkNKd1U1UFAxbnNOemRkU09FSm5kSllITmJicm9tNlpGTGJqdTJRTWtcL2dXcEZBQ2d
ZVjlob0hpT283QkNTaVozZlBDNHRwbWh4T1BxbWRaRFl3SW5TVTBNZ2FZUDNwODAzejJmMTZnMWtnMlRsZHQ0R3JvdWJLaWZmVzRSdW1
Gd3VJUFpaZThES0Q4MzRQUThDQXdFQUFhTmVNRnd3RXdZRFZSMGxCQXd3Q2dZSUt3WUJCUVVIQXdJd1JRWURWUjBCQkQ0d1BJQVF4Zyt
uK2oxakFVMWYyM251UzY1WFBhRVdNQlF4RWpBUUJnTlZCQU1UQ1UxR0lHVXRTMkZ6ZVlJUXM4TFZlWjl1UDVsQWxudlhlOGJZZWpBTkJna3
Foa2lHOXcwQkFRc0ZBQU9CZ1FCWmZrXC9LeEV5XC8zeklmUDByNE50NURnNUxiSjczN2tSZklaUmh1M1BIbU10aEFhYzJrVEx0YWFhV0MraUw
3MG5tOHRcL0o5a1JEOVV5azgzdkxtTGJQR1ZFYmNPbFkrNU9vNVhZZXR1YlNkTEZuTG00a2lGVURoNU5QNEFLelFkVHBDcDRqYkFPV1JGSkNicl
paYlY2TTBYeXRBRVwvbWxyVHJtbDlLMzEzTXhSdz09Il19.hVLbbtNAEP2Vap43sHYubf1maIlKirFIokpBKNraS3F8WWu9rlVH-XdmxkmlQAV-
2fFczjlz2UNq8rbUlYNgD5V6Kkync7I7bZudggA-x4vtIlyG2zj8Fs6_RttnbyRBQKqcwhhm-
NKXIzkZeXIlp4E_DibTd7PLqw0cBNTKqidTEWKtykwnH39ZCDwBzjhVkLtXdbHprEEFvj-

WWNOrfFnbXqf_whYk7O4GgqmAysZEgwACctXsNFLAYjAENC5erSH4voeMEEN0dcoS3Vgi3dE9f3XD5gEOP1C6SZu25FmoonU0i_g-
IsC2VJF2zjDoo23Z9BBOwLMagAWiLgdiZCSW1zwpT3lnWXMmJewPx0yfccgTm5RRD9TrjcEFTUhf_5LQilCEM6idpJ6ryQrTJIjtoWpT01h-
qqLRAhJdqVNSpfqOmovovWCk9oIqzjqgFv5m4V7-x8JJb7L48McEaASVxdW94L-UHp-QScvMOG-
4UKzmaRyBjsEWqO6TeqTNP6xufayV9F1jILqL0Tu7viTHlSRSlVrdMM4e2iJLSNmaXwF4pTvu5wsbpqPuCP6eBg8RvyQr6YejGIxhNWXLKWzgMZ
qUo9zMCNmBN7iusvwNnZW97bLT0b9ntzfzfJzK4Tc.Byu9xqb7YUehEhkJphBj6XrJQ5ak3eAic3xbeGbrPDjjDZdQzOXH-DikjMhRr5gIJQatZZ-
R5QIRWOUor2sYw0jOIpp1g5L5F_yGWputFLDOUK5qF8nvZKFnknAL_CD51ie7rumKSevE7TmvIk736RPD01FIRiu-rSg0Kic-
4qTdTekEI9UbDaOAnHnkMNGhEsam9pv4F4sSpy9ronoDEs4S-SGAParwqzy-AZ8XqmUBl6w5p_X6N8fNjK-
lzh3su5VmRDo8JbfkAS3S7sz4VUTr8Sifow2woSjQYXXOeqf1x2ZCJzgCv5AntpR5sHzhMNA4Pb48OgrIPKYmthEU9g

C.3.6c Pełna postać obiektu JWS paragonu fiskalnego w postaci elektronicznej (trzeciego):

eyJlUGFyYWdvbi5tZi5nb3YucGwiOiJleUozWlhKemFtRWlPaUpLVUV0ZlMwRlRRVjlRUVZKQlIwOU9YM1l4TFRBaUxDSktVRXRKUkNJNklqQXdN
VEF3TURBd01EQXdNREF3TURBd055SXNJbVJoZEdGS1VFc2lPaUl5TURJd0xUQTBMVEV3VkRBM09qSXpPalExTGpZM09Gb2lMQ0pLVUV0U1JV
WWlPbnNpVTBoQk1qVTJJam9pTnpjMk9VTXpPRGxDUWpNelF6ZEdNelJDTURaRU1VTkNOa013UkVFeE0wWTVRVVF6TURVNE5VSkdSVFEzU
WpkRVFqQTROVUV5UVRJMk9Ea3dSVEV3TVNJc0lrcFFTMGxFSWpvaU1EQXhNREF3TURBd01EQXdNREF3TURBMUluMTkiLCJhbGciOiJSUzI1Ni
IsImpwa21ldGFkYXRhIjoiZXlKamIyMXdjbVZ6YzJsdmJpSTZJa1JGUmt4QlZFVWlmUT09IiwieDVjIjpbIk1JSURLakNDQXBPZ0F3SUJBZ0lRMjd1b2xJ
cERIS2RBSmpMU0FIRDQrekFOQmdrcWhraUc5dzBCQVFzRkFEQVVNUkl3RUFZRFZRUURFd2xOUmlCbExVdGhjM2t3SGhjTk1qQXdNekUyTVRB
ek5UVTVXaGNOTWpVd016RTJNVEF6TlRVNFdqQ0JyakVqTUNFR0ExVUVDeE1hUkdWd1lYSjBZVzFsYm5RZ1NXNW1iM0p0WVhSNWVtRmphb
Wt4SGpBY0JnTlZCQW9URlUxcGJtbHpkR1Z5YzNSM2J5QkdhVzVoYm5OdmR6RVpNQmNHQTFVRUJSTVFWa0ZVVVV3dE5qazNNREF3TURnd0
1qRVdNQlFHQTFVRUF4TU5WMVJGTWpBd01UQXdNREF3T1RFUk1BOEdBMVVFQnhNSVYyRnljM3BoZDJFeEZEQVNCZ05WQkFnVEMwMWhl
bTkzYVdWamEybGxNUXN3Q1FZRFZRUUdFd0pRVERDQ0FTSXdEUVlKS29aSWh2Y05BUUVCQlFBRGdnRVBBRENDQVFvQ2dnRUJBTHRTSDdBd
1NPVDRxVDg2M0JBd2J0MkR2R3FFZ0ROVlwvZzBkdFdLODFDNXZLNjc3bWI5WTdVMFBjY1JKRzRodDdCK2ttUnZmc085MllnbmptcFFFcUFKajR
HeUNpY0dYYUkrNmY2eGVVUWtud3ZwQUh2cG1QR3ZaamxzQW1IeVNjTGRHcU9YelFncnhWXC9XRTY0akpnZW5kY3Vjc0d1NkFaSFJDVzdyeE
dNQXhHQTJ5U2dFcE5aQlFxOGhwaGw3c0FqajBQSFpDSndVNVBQMW5zTnpkZFNPRUpuZEpZSE5iYnJvbTZaRkxianUyUU1rXC9nV3BGQUNnW
VY5aG9IaU9vN0JDU2laM2ZQQzR0cG1oeE9QcW1kWkRZd0luU1UwTWdhWVAzcDgwM3oyZjE2ZzFrZzJUbGR0NEdyb3ViS2lmZlc0UnVtRnd1S
VBaWmU4REtEODM0UFE4Q0F3RUFBYU5lTUZ3d0V3WURWUjBsQkF3d0NnWUlLd1lCQlFVSEF3SXdSUVlEVlIwQkJENHdQSUFReGcrbitqMWp
BVTFmMjNudVM2NVhQYUVXTUJReEVqQVFCZ05WQkFNVENVMUdJR1V0UzJGemVZSVFzOExWZVo5dVA1bEFsbnZYZThiWWVqQU5CZ2txaG
tpRzl3MEJBUXNGQUFPQmdRQlpma1wvS3hFeVwvM3pJZlAwcjROdDVEZzVMYko3MzdrUmZJWlJodTNQSG1NdGhBYWMya1RMdGFhYVdDK2
lMNzBubTh0XC9KOWtSRDlVeWs4M3ZMbUxiUEdWRWJjT2xZKzVPbzVYWWV0dWJTZExGbkxtNGtpRlVEaDVOUDRBS3pRZFRwQ3A0amJBT1d
SRkpDYnJaWmJWNk0wWHl0QUVcL21sclRybWw5SzMxM014Unc9PSJdfQ.hVJtb5tADP4rlT9ftoNmScs3tnZRl46hJVGlTFPkwq0jvBw6jqIS5b_P
PmikdtX2CeOznxfbB0h13paqshAcoMKHQncq57hTptkjBPAlXu6W4SrcxeH3cPEt2j16EwkCUrRIb1ThS19O5HTiybWcB_55MP3wbja_2MJRQI0G
H3TFiDWWmUo-
_TYQeAKstlhwuse62HZGkwLfP5eSmnrMV7XpVfovcMHKbq4gmAuoTMw8EEwF5NjsFXHAcggENDZebyD4cYCMEUNKdWiYz9GN6cUpDds7OP
4k7Tpt2tINA4vW8jDi24gB2xIjZa12oPemdaHHcAIecUQWhLsaqImTeU6VUp4qX5QtHC_DfxxL_QGJU7FOnyWT4StNa5qxyP4p4UWREqvJAOt9J
SkrdJMQvEfadc3D-YVFowQkqsJTVYV9xx4j_p45rPaMW17YYB9_8wyG_sczVL3J48OrOfAgKkM7fKJ_KT13TDotM2294Vap241kBBofW-C-
z3jPJ3C3vvapl3nlJT1ENzFlZ5dzTlxIJsXUqMbhHKAtsoSVbdxXAN3r3hn66gLdsT2Gv-XhQ-S-LCvph-sYgmE9ZetKXEBXqVP36sxMiB3cFjdVlr-
hszLXXfZ8_e9d2pt5Pk3l-Ac.coZL-RnBrdTg9Z2fi7heBuQrL8yaKACI7mvUu7ox0h1MJqo9HNKigYupzXz_q54j8bYN4qm5n6FS-
qQ6wCMfz4mRf_HGfxp1fQG3FM7RvB6RAtOgkwywqA77RZuqISP_a4IemcijpL2z2uoqBO2VqB8OSAIPzQ7YwBJWBmGD2WS0ztEZGpqcFBpW
PZhyW1Kw0CvI6JeynHWTgegLGNpj23Z9VSIvmSoBKwX7z0kpWd0jD4BtMX5CrNDiDcmh5Q04TOy8P69E8nDrJZj7HBBKEGzX8LRTO3jQqfuJxH
HtDfGb-xZXOmfRv9XCtRrb4mMD2wjJR8NQu3GQasYznoeQlQ

C.3.6d Pełna postać obiektu JWS paragonu fiskalnego w postaci elektronicznej (czwartego):

eyJlUGFyYWdvbi5tZi5nb3YucGwiOiJleUozWlhKemFtRWlPaUpLVUV0ZlMwRlRRVjlRUVZKQlIwOU9YM1l4TFRBaUxDSktVRXRKUkNJNklqQXdN
VEF3TURBd01EQXdNREF3TURBd09DSXNJbVJoZEdGS1VFc2lPaUl5TURJd0xUQTBMVEV3VkRBNE9qSXpPalExTGpZM09Gb2lMQ0pLVUV0U1JV
WWlPbnNpVTBoQk1qVTJJam9pUWtKR05ETkVRVGhHTVVKQ016RkJSVFpHTXpFME9Ua3dOVGN6TWtNMU1FRkVOMEU0T0VKRE5rRXlRMFV
5UVRrek5qQkNORFZEUWtNeFEwUkRSakJHTVNJc0lrcFFTMGxFSWpvaU1EQXhNREF3TURBd01EQXdNREF3TURBM0luMTkiLCJhbGciOiJSUzI1
NiIsIng1YyI6WyJNSUlES2pDQ0FwT2dBd0lCQWdJUTI3dW9sSXBESEtkQUpqTFNBSEQ0K3pBTkJna3Foa2lHOXcwQkFRc0ZBREFVTVJJd0VBWUR
WUVFERXdsTlJpQmxMVXRoYzNrd0hoY05NakF3TXpFMk1UQXpOVFU1V2hjTk1qVXdNekUyTVRBek5UVTRXakNCcmpFak1DRUdBMVVFQ3hN
YVJHVndZWEowWVcxbGJuUWdTVzVtYjNKdFlYUjVlbUZqYW1reEhqQWNCZ05WQkFvVEZVMXBibWx6ZEdWeWMzUjNieUJHYVc1aGJuTnZkek
VaTUJjR0ExVUVCUk1RVmtGVVVFd3ROamszTURBd01EZ3dNakVXTUJRR0ExVUVBeE1OVjFSRk1qQXdNVEF3TURBd09URVJNQThHQTFVRUJ4T
UlWMkZ5YzNwaGQyRXhGREFTQmdOVkJBZ1RDMDFoZW05M2FXVmphMmxsTVFzd0NRWURWUVFHRXdKUVREQ0NBU0l3RFFZSktvWklodm
NOQVFFQkJRQURnZ0VQQURDQ0FRb0NnZ0VCQUx0U0g3QXdTT1Q0cVQ4NjNCQXdidDJEdkdxRWdETlZcL2cwZHRXSzgxQzV2SzY3N21iOVk3V
TBQY2NSSkc0aHQ3QitrbVJ2ZnNPOTJZZ25qbXBRRXFBSmo0R3lDaWNHWGFJKzZmNnhlVVFrbnd2cEFIdnBtUEd2Wmpsc0FtSHlTY0xkR3FPWH
pRZ3J4VlwvV0U2NGpKZ2VuZGN1Y3NHdTZBWkhSQ1c3cnhHTUF4R0EyeVNnRXBOWkJRcThocGhsN3NBamowUEhaQ0p3VTVQUDFuc056ZGR
TT0VKbmRKWUhOYmJyb202WkZMYmp1MlFNa1wvZ1dwRkFDZ1lWOWhvSGlPbzdCQ1NpWjNmUEM0dHBtaHhPUHFtZFpEWXdJblNVME1nY
VlQM3A4MDN6MmYxNmcxa2cyVGxkdDRHcm91YktpZmZXNFJ1bUZ3dUlQWlplOERLRDgzNFBROENBd0VBQWFOZU1Gd3dFd1lEVlIwbEJBd3d
DZ1lJS3dZQkJRVUhBd0l3UlFZRFZSMEJCRDR3UElBUXhnK24rajFqQVUxZjIzbnVTNjVYUGFFV01CUXhFakFRQmdOVkJBTVRDVTFHSUdVdFMyRn
plWUlRczhMVmVaOXVQNWxBbG52WGU4YlllakFOQmdrcWhraUc5dzBCQVFzRkFBT0JnUUJaZmtcL0t4RXlcLzN6SWZQMHI0TnQ1RGc1TGJKN
zM3a1JmSVpSaHUzUEhtTXRoQWFjMmtUTHRhYWFXQytpTDcwbm04dFwvSjlrUkQ5VXlrODN2TG1MYlBHVkViY09sWSs1T281WFlldHViU2RM
Rm5MbTRraUZVRGg1TlA0QUt6UWRUcENwNGpiQU9XUkZKQ2JyWlpiVjZNMFh5dEFFXC9tbHJUcm1sOUszMTNNeFJ3PT0iXX0.eyJkb2t1bWVu
dCI6eyJuYWdsb3dlayI6eyJ3ZXJzamEiOiJKUEtfS0FTQV9QQVJBR09OX3YxLTAiLCJkYXRhSlBLIjoiMjAyMC0wNC0xMFQwODoyMzo0NS42NzhaIn
0sInBhcmFnb24iOnsicGFtaWVjQ2hyIjoxLCJ0b3RhbCI6eyJ6YXBsWndyb3QiOjIyMzAwfSwiemFrU3ByemVkIjoiMjAyMC0wNC0xMFQwODoyMz
o0NS42NzhaIiwiSlBLSUQiOjgsIm5yUGFyYWciOjUsImthc2plciI6Ikthc2plciIsInN0UFRVIjpbeyJpZCI6IkEiLCJ3YXJ0IjoyMzAwfSx7ImlkIjoiRyIsIndhc

nQiOiJaVyJ9XSwicG9kc3VtIjp7IndhbHV0YSI6IlBMTiIsInN1bWFOZXR0byI6W3siYnJ1dHRvIjoxMjMwMCwidmF0IjoyMzAwLCJpZFN0UFRVIjoiQSJ9LHsiYnJ1dHRvIjoxMDAwMCwidmF0IjowLCJpZFN0UFRVIjoiRyJ9XSwic3VtYUJydXR0byI6MjIzMDAsInN1bWFQb2QiOjIzMDB9LCJuckRvayI6NywicG96eWNqYSI6W3sidG93YXliOnsiYnJ1dHRvIjoxMjMwMCwiaWxvc2MiOiIxIiwib3BlciI6ZmFsc2UsImNlbmEiOjEyMzAwLCJuYXp3YSI6Ik5hendhIHRvd2FydSAxIiwiaWRTdFBUVSI6IkEifX0seyJ0b3dhciI6eyJicnV0dG8iOjEwMDAwLCJpbG9zYyI6IjEiLCJvcGVyIjpmYWxzZSwiY2VuYSI6MTAwMDAsIm5hendhIjoiTmF6d2EgdG93YXJ1IDIiLCJpZFN0UFRVIjoiRyJ9fV0sIm5yS2FzeSI6IjAwMSJ9LCJwb2RtaW90MSI6eyJuYXp3YVBvZCI6Ik5hendhIHBvZG1pb3R1IiwibnJGYWJyIjoiV1RFMjAwMTAwMDAwOSIsIk5JUCI6IjY5NzAwMDA4MDIiLCJhZHJlc1BvZCI6eyJ1bGljYSI6IlVsaWNhIiwibWllanNjIjoiTWllanNjb3dvc2MiLCJuckxvayI6Ik5yTG9rIiwicG9jenRhIjoiUG9jenRhIiwibnJEb211IjoiTnJEb211Iiwia29kUG9jenQiOiIwMC0wMDAifSwibnJVbmlrIjoiV1RFMjAwMTAwMDAwOSIsIm5yRXdpZCI6IjIwMjAvMDAwMDAxNjEyIn19fQ.sXtOYl09QSQpRre0SJM9nLalPLu-6R5gL-VPGE37SbMASEHmMs4ZxmmCc-YjLgimJyL4gRbyI8A5PwdSSZ5OH4zHW4xdGftBlPyhbniubjJ43rVxq0-R1Sdj3mDyzIIm1rJeflYHdfYD1Y2IKcyT3Yuv9dsTSjtCAqrOKUGoY-EnGhEfo5dcaV7LHZxQm7trjL_wrunKP3e3S_anzQNf2pW4nqpCHBwBKBGs7kkB1wPcoh3exUhjodVGkuGAVCABvuQ_Zc9wySc3aPtFUrPj5vgeg1BEu-mt58dzcqW9YfoCrwWBZnh7gBbDeOzrnjKEKHtzv3W0Wa9qd89HdcsTEg