Техническа спецификация за обмен на данни между участници на пазара на електрическа енергия

Приложение №6 - Комуникационна свързаност и технически начин за обмен на данни

Документ: Приложение 6

Версия: 1.0

Дата на издаване: 31.01.2019

**ИСТОРИЯ НА ПРОМЕНИТЕ:**

|  |  |  |
| --- | --- | --- |
| **Дата** | **Кратко описание на промените** | **Версия** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Комуникационна свързаност и технически начин за обмен на данни:**

1. **Цели на комуникационната разработка**
   1. На Операторите на Разпределителни Мрежи (ОРМ) и на Независимият Преносен Оператор (НПО) да се осигури сигурно, достъпно и скалируемо решение за обмен на данни, в контекста на Инструкцията, наричано още „информационна среда“ в настоящото Приложение;
   2. На Доставчиците на Електрическа Енергия (ДЕЕ) и Координаторите на Балансиращи Групи (КБГ) да се осигури лесен и сигурен достъп до информационната среда, посредством широко използвани инструменти и съвременни технологии;
   3. Всички необходими елементи за изграждането на информационната среда по смисъла на настоящото Приложение да е възможно да бъдат осигурени чрез ползване на безплатен софтуер с отворен код. В същото време всеки един от участниците в процеса по обмен на данни може да използва софтуерно или хардуерно решение по негов избор, което би осигурило необходимата функционалност, независимо от вид, произход или производител.
2. **Протокол за комуникация – HTTPS, транспортен слой**
   1. Операторите на разпределителни и преносни мрежи се задължават да изградят информационна среда, представляваща web-базирано сървърно решение, което използва само HTTPS (Hypertext Transfer Protocol Secure) протокол за обработка на клиентски заявки. TCP порта за HTTPS да отговаря на стандартите по RFC, т.е. да се ползва TCP/443;
   2. Операторите на разпределителни и преносни мрежи се задължават да осигурят TLS (Transport Layer Security) комуникация, която да е с версия 1.1 или по-висока. Задължително е инсталирането и използването на SSL (Secure Socket Layer) сертификат, издаден от CA (Certificate Authority), включено в „Trusted Root Certificate Program“ и с минимални параметри: signature algorithm SHA256 ECDSA; частен ключ (Private Key), издаден с RSA и с дължина не по-малка от 4096 бита; валидност на сертификата не по-малко от 2 години;

*Примерен начин за генериране на частен ключ:*

shell>openssl genrsa -out host.operator.domain.key 4096

*Примерен начин за генериране на CSR към CA:*

shell>openssl req -new -key host.operator.domain.key -out host.operator.domain.csr

*При генериране на частен ключ и CSR за издаване на сертификат е задължително да се прегледат техническите препоръки на съответното CA.*

* 1. Доставчиците на ел. енергия и Координаторите на балансиращи групи са клиенти на информационната среда, осигурена от Операторите по смисъла на 2.1 и 2.2. Всеки един от участниците в обмена на данни се задължава да генерира и използва самоподписан клиентски сертификат (self-signed certificate), с минимални параметри: signature algorithm SHA256 ECDSA; частен ключ (Private Key), издаден с RSA и с дължина не по-малка от 4096 бита; валидност на сертификата не по-малко от 2 години;
  2. Операторите на мрежи обменят данни по между си посредством същата информационна среда;
  3. Публичният ключ (Public Key) на издаденият сертификат по т. 2.3 трябва да бъде подаден на всички Оператори на разпределителни и преносни мрежи посредством удостоверителен начин – онлайн чрез използване на електронна поща, подписана чрез валиден УЕП на законен представител на съответното Юридическо лице, или лично – в централния офис на всеки един от Операторите, съответно от страна на упълномощен представител;
  4. Надеждното съхранение на частните ключове (Private Keys) е отговорност за всеки един от участниците;
  5. Не се предават данни от и към участник в обмена в случая на изтекъл сертификат или неотговарящ на точка 2.2. и 2.3. В този случай се пристъпва към повторно изпълнение на т. 2.2. и 2.3.

*Примерен начин за създаване на slef-signed certificate:*

shell>openssl req -newkey rsa:4096 -nodes -keyout private-key.pem -x509 -days 730 -out public-certificate.pem -subj '/CN=EIC-VALID-NUMBER/O=Client-Name/OU=Unit-Description/C=BG'

*Файлът public-*certificate.pem *е предмет на предаване към Операторите на разпределителни и преносни мрежи по реда, описан в т. 2.5 от настоящата инструкция. Издаденият клиентски сертификат, при необходимост трябва да се конвертира във вид, използваем от съответното клиентско приложение.*

*EIC-VALID-NUMBER е съответният EIC код на участника, издаден от НПО, Client-Name е името на Юридическото лице а Unit-Description е поле, което позволява да се специфицира допълнителна информация за конкретният офис или структура на Участника, която ще ползва сертификата.*

1. **Протокол за комуникация HTTPS – приложен слой**
   1. Автентификацията на доставчиците на ел. енергия и координатори на балансиращи групи пред информационната среда за обмен на данни на операторите на електроразпределителните и преносни мрежи се осъществява чрез подаване на потребителско име и парола (username, password), като същата се извършва само и единствено посредством вече изградена TLS 1.x комуникация между страните. Използва се HTTP Basic Authentication. Authentication headers се изпращат при всяка заявка, описана в т. 3.6.
   2. Потребителското име е EIC кода на участника на пазара, издаден от НПО.
   3. Всяка една от системите на участниците на пазара трябва да издава и изпраща инициализираща парола чрез електронна поща или SMS до съответният потребител, както и трябва да се осигурява функционалност за смяна на паролата. В системите на Операторите се съхранява hash на паролата, но не и паролата в явен вид.

Паролата трябва да съдържа минимум 10 (десет) символа, от които минимум са 4 букви от латинската азбука и изпълнени следните правила:

* поне една главна буква
* поне една малка буква
* поне една цифра
* поне един специален символ

Последните 5 пароли трябва да са уникални. Период на валидност на паролата – не по-голяма от 180 дена. При получаване на инициализираща парола, потребителят е длъжен да я смени, преди да ползва системата.

* 1. Паролата на един участник не трябва да се споделя с останалите ДЕЕ/КБГ/Оператори, като при съмнения за компрометирането й, незабавно трябва да бъде променена от съответният Потребител в съответната система. Всеки един участник на пазара трябва да поддържа различна парола за достъп до различните системи за обмен на данни.
  2. При реализациите на web сервизите се използват само POST методи за предаване на данни, RFC 7231, Accept-Charset UTF-8, Accept-Encoding: deflate, gzip, Accept-Language bg-BG. Предават се само XML структури.
  3. Всяко ОРМ/НПО следва да предостави входно/изходна точка за комуникация (URL). Обработват се 4 (четири) вида заявки, предназначени за осигуряване на функционалност, както следва:
     1. Заявка за “change password“ (POST), с входен параметър: нова парола. Релативен URL /passwd/ и параметър:

**newpw**: нова парола (задължително поле)

*Примерен начин за смяна на парола:*

shell>curl --cert *public-*certificate.pem --key private-key.pem -u EIC-User-Name:Initial123!@#Password -X POST -F newpw=’Pas$W0rd1234’ https://web.server.domain/passwd/

* + 1. Заявка за “upload” (POST) на XML структура от страна на ДЕЕ или КБГ, с входен параметри: XML съдържание. Релативен URL /upload/ и параметър

**xml**: съдържание на XML (задължително поле)

*Примерен начин за upload на XML документ:*

shell>curl --cert *public-*certificate.pem --key private-key.pem -u EIC-User-Name:Pas$W0rd1234 -X POST -F xml=’@xml2upload.xml’ https://web.server.domain/upload/

или

shell>curl --cert *public-*certificate.pem --key private-key.pem -u EIC-User-Name:Pas$W0rd1234 -X POST -F xml='<xml>content</xml>' https://web.server.domain/upload/

* + 1. Заявка за “download” (POST) на XML структура към ДЕЕ или КБГ, с входни параметри: идентификационен код (unsigned long int) за XML съдържание. Релативен URL /download/ и параметър:

**id**: идентификационен код (задължително поле)

*Примерен начин за download на XML документ:*

shell>curl --cert *public-*certificate.pem --key private-key.pem -u EIC-User-Name:Pas$W0rd1234 -X POST -F id=5 https://web.server.domain/download

* + 1. Заявка за получаване на списък със съобщения “list” (POST), на практика същата като в т. 3.12.2, от страна на сървъра, съдържащ идентификатори на XML структури, готови за “download“. Релативен URL /download/ и параметри:

**id**=0 идентификационен (незадължителен параметър, ако не бъде подаден, по подразбиране се приема id=0);

*Примерен начин за download на XML списък с налични съобщения:*

shell>curl --cert *public-*certificate.pem --key private-key.pem -u EIC-User-Name:Pas$W0rd1234 -X POST -F id=0 https://web.server.domain/download

* + 1. При коректно изпълнена заявка, WEB клиента трябва да получи отговор „HTTP/1.1 200 OK“. При всички останали отговори заявката се счита за неуспешно обслужена.
    2. При некоректно въведено потребителско име или парола WEB клиента получава „403 Forbidden”.
    3. При изтекла по давност парола WEB клиента получава „418“.

*Примерен получен резултат от горната заявка при нормално изпълнение:*

<?xml version="1.0" encoding="UTF-8"?>

<list>

<message id="10"/>

<message id="11"/>

<message id="12"/>

</list>

*съответстващ на следната XML схема:*

<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified" xmlns:xs="<http://www.w3.org/2001/XMLSchema>">

<xs:element name="list">

<xs:complexType>

<xs:sequence>

<xs:element name="message" maxOccurs="unbounded" minOccurs="0">

<xs:complexType>

<xs:simpleContent>

<xs:extension base="xs:string">

<xs:attribute type="xs:long" name="id" use="required"/>

</xs:extension>

</xs:simpleContent>

</xs:complexType>

</xs:element>

</xs:sequence>

</xs:complexType>

</xs:element>

</xs:schema>

* + 1. При ползване на функционалността по 3.6.3, системата на Оператора дава възможност да се изтегли само документа с най-малката стойност на ID. При изтеглянето на този документ, след потвърждение “200 OK”, системата на оператора позволява да се стартира изтегляне на следващият документ, със стойност на ID по-голяма от предходният и по-малка от всички останали. Препоръчително е всички обработки от страна на клиента по първоначално изтегленият документ да са приключени, преди да се генерира заявка за изтегляне на следващ документ.
    2. След изтегляне на XML документ, потвърдено от страна на клиента с “200 OK”, и съответно чрез стартиране изтеглянето на следващият документ по реда, предходният документ бива маркиран за успешно получен и съответно се маркира за премахване от списъка за изтегляне от системата на Оператора. Системите автоматично изтриват успешно изтеглените документи по описаният ред един път на денонощие, в периода 05:00 до 06:00 часа.
    3. Системата на оператора позволява изтегляне и изпращане на документи по смисъла на 3.6. само, ако потребителската парола отговаря на изискването по 3.3. При несъответствие с настоящото, потребителят има достъп само до функционалността, описана в 3.6.1.

# СПИСЪК НА ПРИЛОЖЕНИЯТА

|  |  |  |
| --- | --- | --- |
| **Приложeние №** | **Описание** | **Име на файл** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |