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

Приложение №6 – Комуникационна свързаност и технически способи за обмен на данни

Документ: Приложение 6

Версия: 1.1

Дата на издаване: 30.10.2020

ИСТОРИЯ НА ПРОМЕНИТЕ:

Дата	Кратко описание на промените	Версия
27/10/2020	Актуализиране понятията по темата цифрови сертификати. Прецизиране на текстовете, свързани с връщани грешки по HTTP	1.1

Съдържание

1. ЦЕЛИ НА КОМУНИКАЦИОННАТА РАЗРАБОТКА 4

2. ПРОТОКОЛ ЗА КОМУНИКАЦИЯ HTTPS – ТРАНСПОРТЕН СЛОЙ 5

2.1. Информационна среда 5
2.2. TLS (Transport Layer Security) и SSL (Secure Socket Layer) изисквания – сървърна част 5
2.3. Достъп на КБГ и ДЕЕ до информационната среда 5
2.4. Достъп на МО до информационната среда 5
2.5. Начини на предаване на публичен ключ (Public Key) на клиентски сертификат 5
2.6. Начини на съхранение на частен ключ (Private Key) на клиентски сертификат 6
2.7. Ограничения за използване на информационната среда 6
2.8. Начини за действие при (съмнение за) компрометиране на клиентски сертификат 6

3. ПРОТОКОЛ ЗА КОМУНИКАЦИЯ HTTPS – ПРИЛОЖЕН СЛОЙ 7

3.1. Начин за автентификация пред информационната среда 7
3.2. Изисквания към потребителското име за достъп до информационната среда 7
3.3. Изисквания към паролата за достъп до информационната среда 7
3.4. Начини за действие при (съмнения за) компрометиране на парола за достъп 7
3.5. Изисквания към реализацията на web сервизите 8
3.6. Входно/изходни точки за комуникация (URLs) 8

1. ЦЕЛИ НА КОМУНИКАЦИОННАТА РАЗРАБОТКА

Основни цели на настоящата комуникационната разработка са:

- Да се осигури сигурно, достъпно и скалируемо решение за обмен на данни в контекста на „Инструкция по чл. 88, ал. 3 от ПТЕЕ за единен електронен формат за обмен на данни на пазара на електрическа енергия“ (Инструкцията), наричана още „информационна среда“ на мрежовите оператори (МО);
- Да се осигури сигурен достъп до информационната среда посредством широко използвани инструменти и съвременни технологии на координаторите на балансиращи групи (КБГ) и доставчиците на електрическа енергия (ДЕЕ);
- Да се осъществи възможност да бъдат гарантирани, чрез ползване на безплатен софтуер с отворен код, всички необходими елементи за изграждането на информационната среда, по смисъла на настоящото Приложение 6. В същото време всеки един от участниците в процеса по обмен на данни да може да използва софтуерно или хардуерно решение по негов избор, което би осигурило необходимата функционалност, независимо от вида, произхода или производителя.

2. ПРОТОКОЛ ЗА КОМУНИКАЦИЯ HTTPS – ТРАНСПОРТЕН СЛОЙ

2.1. Информационна среда

МО се задължават да изградят и поддържат информационна среда, представляваща web-базирано сървърно решение, което използва само HTTPS (Hypertext Transfer Protocol Secure) протокол за обработка на клиентски заявки. TCP портът за HTTPS трябва да отговаря на стандартите по RFC 2818, т.е. да се ползва само TCP/443.

2.2. TLS (Transport Layer Security) и SSL (Secure Socket Layer) изисквания – сървърна част

МО се задължават да осигурят TLS (Transport Layer Security) комуникация, която да е с версия 1.2 или по-висока. Задължително е инсталирането и използването на валиден SSL (Secure Socket Layer) сертификат, издаден от CA (Certificate Authority), включено в „Trusted Root Certificate Program“ или включено в регистъра на доставчиците на удостоверителни услуги на КРС (Комисия регулиране на съобщенията). Валидността на сертификата е максимално възможната, съгласно текущите политики, прилагани от съответното CA. Така издаденият сертификат трябва да отговаря на минимум Security Strength 128, съгласно NIST.

2.3. Достъп на КБГ и ДЕЕ до информационната среда

КБГ и ДЕЕ са клиенти на информационната среда, осигурена от всички МО по смисъла на т. 2.1. и т. 2.2. Всеки един от участниците в обмена на данни се задължава да използва клиентски сертификат със задължително попълнени полета O=Organization-Name, OU=Organization-Unit и CN=EIC-VALID-NUMBER. Валидност на сертификата – не по-малко от 1 година и не повече от 2 години.
EIC-VALID-NUMBER е съответният EIC код на участника, издаден от НПО. Не се допуска наличието на друго съдържание в CN. В клиентският сертификат се допуска само един единствен CN, попълнен в “subject dn”.
Така издаденият сертификат трябва да отговаря на минимум Security Strength 128, съгласно NIST.

2.4. Достъп на МО до информационната среда

МО обменят данни по между си посредством същата информационна среда, като всеки един МО се регистрира като клиент пред останалите МО като съответно изпълнява т. 2.3. по отношение изискванията към клиентския сертификат.

2.5. Начини на предаване на публичен ключ (Public Key) на клиентски сертификат

Публичният ключ (Public Key) на издадения клиентски сертификат по т. 2.3. трябва да бъде подаден на всички МО посредством удостоверителен начин: онлайн, чрез използване на електронна поща, подписана с валиден УЕП на законен представител на съответното юридическо лице или лично в офис на всеки един от мрежовите оператори, съответно от страна на упълномощен представител.

2.6. Начини на съхранение на частен ключ (Private Key) на клиентски сертификат

Надеждното съхранение на частните ключове (Private Keys) е отговорност за всеки един от участниците.

2.7. Ограничения за използване на информационната среда

Не се предават данни от и към участник в обмена в случай на изтекъл сертификат или неотговарящ на т. 2.2. и т. 2.3. В този случай се пристъпва към повторно изпълнение на т. 2.2. и т. 2.3.
Задължение на клиента е да проверява при всяко изграждане на TCP сесия за валидността на сървърния сертификат на МО, задължение на МО е да проверява валидността на клиентския сертификат.

2.8. Начини за действие при (съмнение за) компрометиране на клиентски сертификат

При съмнение за компрометиран клиентски сертификат, съответният клиент трябва да информира незабавно всички МО и да предостави нов клиентски сертификат по реда на т. 2.3.
При съмнение за компрометиран клиентски сертификат от страна на МО, последният има право да прекрати достъпа на компрометирания клиентски сертификат до изясняване на случая.

3. ПРОТОКОЛ ЗА КОМУНИКАЦИЯ HTTPS – ПРИЛОЖЕН СЛОЙ

3.1. Начин за автентификация пред информационната среда

Автентификацията в информационната среда за обмен на данни се осъществява чрез подаване на потребителско име и парола (username, password), като същата се извършва само и единствено посредством вече изградена сесия TLS 1.2 (или по-висока версия) за комуникация между страните. Използват се HTTP параметри, указващи потребителско име и парола при подаването на всяка една POST заявка, описана в т. 3.6.

3.2. Изисквания към потребителското име за достъп до информационната среда

Потребителското име е EIC кода на участника на пазара, издаден от независимия преносен оператор (НПО). При процеса на автентификация трябва да се ползва съответният клиентски сертификат, издаден по реда на 2.3, т.е. за същият EIC, подаван и като потребителско име. При несъответствие на подадените EIC (сертификат и потребителско име) системите на МО отхвърлят съответната заявка.

3.3. Изисквания към паролата за достъп до информационната среда

Всяка една от системите на участниците на пазара трябва да издава и изпраща инициализираща, уникална парола чрез електронна поща или SMS до съответният потребител. С тази парола е възможно да се ползва само функционалността, описана в т. 3.6.1. В системите на МО, паролата трябва да се съхранява в неявен вид, чрез ползване на специализирана съвременна hash функция.
Паролата трябва да съдържа минимум 10 (десет) символа, от които минимум са 4 букви само от латинската азбука и изпълнени следните правила:

- поне една главна буква;
- поне една малка буква;
- поне една цифра;
- поне един специален символ, като под специален символ се разбира само някой от следните: !@$^&?/\;
- последните 5 пароли трябва да са уникални.

Дължината на паролата не трябва да надхвърля 16 символа. Периодът на валидност на паролата е не по-голям от 180 дена. След изтекла валидност на паролата не могат да се обменят данни, но може да се смени паролата. При получаване на инициализираща парола, потребителят е длъжен да я смени, преди да ползва системата.

3.4. Начини за действие при (съмнения за) компрометиране на парола за достъп

Паролата на един участник не трябва да се споделя с останалите КБГ/ДЕЕ/МО, като при съмнения за компрометирането ѝ, незабавно трябва да бъде променена от съответният потребител в съответната система. При съмнение за компрометиран акаунт на КБГ/ДЕЕ/МО от страна на съответният МО, последният има право да прекрати достъпа на компрометираният акаунт до изясняване на случая. Всеки един участник на пазара трябва да поддържа различни пароли за достъп до различните системи за обмен на данни.

3.5. Изисквания към реализацията на web сервизите

При реализациите на web сервизите се използват само POST методи за предаване на данни, RFC 7231, Accept-Charset UTF-8, Accept-Language bg-BG. EDIFACT съобщенията се предават само като XML структури. Метаданните в протокола се предават като стрингове с encoding UTF-8.
Реализират се двата начина за предаване на параметри с метод POST – Content-Type: application/x-www-form-urlencoded (RFC 1866) и Content-Type: multipart/form-data (RFC 2388).
Други HTTP заявки (методи), освен POST, не се поддържат. За такива заявки, ползващи други методи, се връща отговор: 405 Method Not Allowed.
За идентификатор на всяко XML съобщение (XML документ) се използва UUIDv4 (RFC 4122) като стойността се съхраня в DOCUMENTNUMBER tag. Същият идентификатор на съобщението се използва за подаване на входен параметър msg_id при сервизите за трансфер на съобщението.
Алгоритъмът за пресмятане на hash сумите на XML съобщенията е SHA-256 – RFC 4634. В пресмятанията на даден hash се включва само съдържанието на съответната XML структура от съобщението.

При реализацията и последващата експлоатация на така описаният протокол, web сервизите и техните клиенти трябва да прилагат общоприетите добри практики за нормално и отговорно поведение в Интернет, като:

- не се ползват инструменти за генериране на злоумишлен трафик към HTTPS (TCP/443) с или без валиден/регистриран клиентски сертификат;
- не се ползват техники за генериране на „flood“ от входящи заявки при вече изградена TLS 1.2 сесия чрез валиден и регистриран клиентски сертификат;
- не се ползват техники за нерегламентиран (недоговорен между страните) одит (независимо дали последният е добронамерен) на сигурността, целящи намиране на „пробив“ в реализацията на дадена система;
- не се структурират и изпращат злоумишлено заявки, различни от така формулираните в настоящият документ;
- не се структурират и изпращат към клиентите на системите злоумишлено невалидни отговори на съответните им заявки.

В случаи на настъпили по така описаните (или сходни) обстоятелства, засегнатият участник веднага трябва да уведоми неизрядната страна (ако е приложимо), като при еднозначна идентификация на зловредният източник и двете страни трябва да предприемат незабавни действия с оглед преустановяване на констатираното поведение.

В случай на констатирано зловредно или злонамерено поведение, което би компрометирало гарантирането на нормалната работата на други потребители със съответната система, всеки МО има правото да предприема технически мерки за противодействие, прилагани по негово усмотрение.

3.6. Входно/изходни точки за комуникация (URLs)

Всеки МО следва да предостави единна входно/изходна точка за комуникация (Base URL от вида https://web.server.domain/base-url/). Base URL трябва да бъде публикувано в общодостъпна част на неговият Интернет сайт. Системата предоставя следните услуги, предназначени за осигуряване на функционалности за обмен на XML съобщения, както следва:

3.6.1. Сервиз за смяна на парола

Метод: POST
Релативен URL: **/password/**
Входни параметри:

- username: (задължително поле) – потребител;
- password: (задължително поле) – текуща парола;
- newpassword (задължително поле) – нова парола.

Примерен начин за смяна на парола:

shell>curl --cert public-certificate.pem --key private-key.pem –F username='EIC-valid-username' –F password='current_password' –F newpassword='new_password' -X POST https://web.server.domain/password/

Сервизът връща един от следните статус кодове:

- 200 OK – новата парола е възприета от системата и в тялото на съобщението се връща до кога ще е валидна, форматът е Unix Timestamp – секунди от 1970-01-01;
- 401 Unauthorized – сертификатът е изтекъл или не отговаря на условията на т. 2.3/ т. 2.4, потребителят или паролата са невалидни;
- 409 Conflict – новата парола е същата като текущата парола или е някоя от последните 5 използвани пароли;
  406 Not Acceptable – не отговаря на изискванията на т. 3.3. В тялото на съобщението присъства информация защо новата парола не е приета.

Примери:

- Not Acceptable – your password is same as your current password;
- Not Acceptable – your password must have at least one special character;
- Not Acceptable – this password is recently used.

3.6.2. Сервиз за upload на XML съдържание

Метод: POST
Релативен URL: **/upload/**
Входни параметри:

- username: (задължително поле) – потребител;
- password: (задължително поле) – текуща парола;
- msg_id: (задължително поле) – уникален идентификатор на изпращаното съобщение от клиента;
- xml: (задължително поле) – съдържание на XML.

Примерен начин за upload на XML документ:

shell>curl --cert public-certificate.pem --key private-key.pem -X POST –F username='EIC-valid-username' –F password='current_password' -F xml='@xml2upload.xml' -F msg_id='83017a7a-e08a-4f30-9a82-5c11ede44a30' https://web.server.domain/upload/

или

shell>curl --cert public-certificate.pem --key private-key.pem -X POST –F username='EIC-valid-username' –F password='current_password' -F xml='<xml>content</xml>' -F msg_id='83017a7a-e08a-4f30-9a82-5c11ede44a30'

Сервизът връща един от следните статус кодове:

- 200 OK – съдържанието на съобщението е качено успешно и валидно спрямо съответната .XSD схема. Ако вече има качено съобщение с този идентификатор (msg_id), като същото не е потвърдено чрез сервиза от 3.6.3, то новото съобщение замества предходното;
- 401 Unauthorized – сертификатът е изтекъл или не отговаря на условията на т. 2.3/ т. 2.4, потребителят или паролата са невалидни;
- 403 Forbidden – вече съществува съобщение с този идентификатор (msg_id) и същото е потвърдено чрез сервиза от т. 3.6.3. При наличие на непотвърдено съобщение с друг (различен от текущо подадения msg_id) идентификатор сервизът връща идентификатора на непотвърденото предходно съобщение;
- 406 Not acceptable – съдържанието на съобщението не е валидно спрямо съответната .XSD схема или DOCUMENTNUMBER tag е с различна стойност от тази на входния параметър msg_id на POST метода.

Сервизът връща hash на полученото XML съобщение при статус 200 OK и статус 406 Not acceptable. Полученият по този начин hash се използва за удостоверяване в сервиза за потвърждение 3.6.3.

Последващ upload на друг XML документ може да бъде осъществен само след потвърждаване на текущия чрез сервиза, описан в т. 3.6.3

3.6.3. Сервиз за потвърждение на изпратено съобщение (upload)

Метод: POST
Релативен URL: **/confirm-upload/**
Входни параметри:

- username: (задължително поле) – потребител;
- password: (задължително поле) – текуща парола;
- msg_id: (задължително поле) – уникален идентификатор на качено от клиента съобщение;
- msg_hash: (задължително поле) hash сума на XML съдържанието, пресметнато от клиента. Hash сумата се предава като стринг, като всеки байт е представен в шестнадесетична бройна система.

Примерен начин за потвърждаване на изпратен XML документ:

shell>curl --cert public-certificate.pem --key private-key.pem -X POST –F username='EIC-valid-username' –F password='current_password' -F msg_hash='28ed9227e73e1cf1c11dff4c97a253139889c7a1d98448355e1e7cb323ea8041' -F msg_id='83017a7a-e08a-4f30-9a82-5c11ede44a30' https://web.server.domain/confirm-upload/

Сервизът връща един от следните статус кодове:

- 200 OK –има успешно записано и потвърдено съобщение от този клиент с подадените идентификатор msg_id и hash msg_hash. С настоящото се приема, че това, което е получила системата на съответният МО е съдържанието, което клиентът е изпратил. При следващ опит за качване на XML съобщение със същия идентификатор чрез сервиза /upload/ от т. 3.6.2. системата ще връща 403 Forbidden;

- 401 Unauthorized – сертификатът е изтекъл или не отговаря на условията на т. 2.3/ т. 2.4, потребителят или паролата са невалидни;
- 403 Forbidden – msg_hash hash на съобщението с идентификатор msg_id не е този, който е пресметнат от системата;
- 404 Not found – няма качено съобщение с такъв идентификатор.

При опит за потвърждаване на hash, който връща статус 403, задължение на клиента е да пристъпи към повторно изпълнение на /upload/ на съответният документ, със същия идентификатор.

3.6.4. Сервиз за download на XML съдържание

Метод: POST
Релативен URL: **/download/**
Входящи параметри:

- username: (задължително поле) – потребител,
- password: (задължително поле) – текуща парола

Настоящата заявка връща винаги първото налично и непотвърдено съобщение за изтегляне. Съобщението се връща като .XML файл. В отговора от сървъра присъстват следните headers:

Content-Type: application/xml; charset=UTF-8
Content-Disposition: attachment; filename="<unique id of the message>"

<unique id of the message> е уникалния идентификатор на съобщението, който съвпада с DOCUMENTNUMBER tag от съдържанието на XML съобщението. Този идентификатор ще се използва със следващата заявка от т. 3.6.5

Примерен начин за download на XML документ изпратен с уникален идентификатор '8df03ccd-f89e-41c7-b7c1-8555748f660b' :

shell>curl --cert public-certificate.pem --key private-key.pem -X POST –F username='EIC-valid-username' –F password='current_password' https://web.server.domain/download

След получаване на съобщението е наличен файл с име: 8df03ccd-f89e-41c7-b7c1-8555748f660b.xml. Получателят пресмята hash сумата на съдържането на съобщението. Полученият hash се връща в стринг, като всеки байт е представен в шестнадесетична бройна система.

Примерен начин за пресмятане на hash:

Shell> sha256sum 8df03ccd-f89e-41c7-b7c1-8555748f660b
f9f6a90c74a2b76c1f3ef3a3e66c7d1d84f6eec35c2c4b78f0581e2b5e52bf2e 8df03ccd-f89e-41c7-b7c1-8555748f660b

Полученият по този начин hash се използва за удостоверяване в сервиза за потвърждение по т. 3.6.5.
Повторното изпълнение на същата заявка, без преминаване през т. 3.6.5 ще връща същото .XML съобщение и същия идентификатор.

Сервизът връща един от следните статус кодове:

- 200 OK – успешно изпълнение – съобщението е изпратено;

- 401 Unauthorized – сертификатът е изтекъл или не отговаря на условията на т. 2.3/ т. 2.4, потребителят или паролата са невалидни;
- 204 No content – няма повече съобщения за получаване.

3.6.5. Сервиз за потвърждение на получено съобщение (download)

Метод: POST
Релативен URL: **/confirm-download/**
Входящи параметри:

- username: (задължително поле) – потребител;
- password: (задължително поле) – текуща парола;
- msg_id: (задължително поле) – съдържа уникалния идентификатор на съобщението, получено чрез сервиза /download/ – т. 3.6.4;
- msg_hash: (задължително поле) – съдържа пресметната hash сума от страна на клиента на полученото съдържание. Сумата се изпраща като стринг, като всеки байт е представен в шестнадесетична бройна система.

Сервизът /confirm-download/ се използва след като клиентът е валидирал полученото XML съобщение спрямо съответната .XSD схема, получено по т. 3.6.4.

Примерен начин за потвърждаване на съобщение:

shell>curl --cert public-certificate.pem --key private-key.pem -X POST –F username='EIC-valid-username' –F password='current_password' -F msg_id='8df03ccd-f89e-41c7-b7c1-8555748f660b' –F msg_hash='f9f6a90c74a2b76c1f3ef3a3e66c7d1d84f6eec35c2c4b78f0581e2b5e52bf2e' https://web.server.domain/confirm-download/

Сервизът връща един от следните статус кодове:

- 200 OK – успешно изпълнение – съобщението е потвърдено. Клиентът може да получи следващото съобщение, като извика сервиза /download/;
- 401 Unauthorized – сертификатът е изтекъл или не отговаря на условията на т. 2.3/ т. 2.4, потребителят или паролата са невалидни;
- 403 Forbidden – hash сумите не съвпадат. Клиентът трябва да се опита да получи съобщението отново чрез сервиза /download/, да пресметне hash сумата на ново-полученият документ и да опита отново да го потвърди, чрез /confirm-download/;
- 404 Not Found – в системата няма съобщение с идентификатор 'msg_id.