УТВЪРДИЛ:
АПОСТОЛ АПОСТОЛОВ

08.02.08

Технологична процедура за обмен на съобщения между КФН и информационни посредници с цел въвеждане на данни в електронния регистър на КФН

1 Въведение

Този документ описва технологичната процедура за електронен обмен на данни чрез връзка от тип "система-система" между Комисията за финансов надзор (КФН) и лицата, които са оправомощени от емитента да разпространяват на обществеността регулираната информация съгласно чл. 43в от Наредба № 2 за проспектите при публично предлагане и допускане до търговия на регулиран пазар на ценни книжа и за разкриването на информация от публичните дружества и другите емитенти на ценни книжа (Наредба № 2) във връзка със задълженията на емитентите за разкриване на регулираната информация по чл. 27, ал.1 от Наредба № 2 и на КФН .

Този интерфейс може да се използва от всички лица, които са оправомощени от емитента да предоставят на КФН регулирана информация и едновременно с това да я разкриват на обществеността съгласно чл. 43в от Наредба № 2, наричани по-нататък "информационни посредници".

Този интерфейс е предназначен за обмен на съобщения относно информацията по чл.27, ал.1 от Наредба №2. Чрез интерфейса се обменят и протоколни съобщения за потвърждение на обмена на съобщенията, както и за обработката на грешките. Съобщенията ще са във формат XML, описан в Приложение 1.

Интерфейсът е за работа в реално време. Комункацията между точките на обмен се криптира и обменяните съобщения са цифрово подписани. Това осигурява да няма загуба на данни, повторение на данни, както и конфиденциалност на обменяната информация.

КФН своевременно уведомява информационните посредници при промяна на образците на електронните форми, които служат за подаване на информация и им ги предоставя в срок не по-късно от 3 дни от одобряването им.

Информационните посредници са длъжни да уведомят незабавно КФН:

- при възникване на технически проблеми, свързани с обмена на данни между тях и КФН;

- при прекратяване на дейността си.

КФН може да прекрати използването на връзката от информациония посредник, когато той системно нарушава изискванията на Правилата, процедурите и стандартите за организация, функциониране и управление на единната система за предоставяне на информация e-Register и настоящата процедура.

1.1 Описание на обменяните данни

Обменяните данни ще съдържат няколко предварителни съобщения за установяване на връзка между системите, няколко XML формат съобщения и допълнителни ACK/NAK съобщения за синхронизация между двете системи.

2 Описание на интерфейса

2.1 Източник и получател

Страните по обмена на данни ще са КФН от една страна и Информационния посредник /ИА/ от друга.

2.2 Тип на интерфейса

Интерфейсът работи в режим на реално време на обработка на получените съобщение без операторска намеса.

За целта е необходимо да се спазва точно протокола на обмен на данни.

Комуникацията ще се инициира като SSLSocket приложение, което да поддържа криптиране на обменяните данни и автентификация на клиента.

За получаване на изпращаните съобщения КФН ще поддържа SSLServerSocket приложение. Получаването на отговорите на КФН на подадените съобщения от ИА ще става веднага в момента на подаването, а генерираните от КФН към ИА съобщения ще се получват при заявка или веднага при активен комуникационен канал. За целите на коректната обработка на информацията ще се използва един канал за обмен на данни . Каналът ще е сървърен процес в системата на КФН на порт 9001 и ще се използва за контролен /управляващ канал и за обмен на съобщения.

Стандартът за SSL комуникация е TLS 1.0.

Информационните посредници използващи този протокол трябва да разполагат с цифрови сертификати за универсален електронен подпис за автентификация пред системите на КФН. SSLSocket сесията ще се инициализира като се използват цифрови сертификати на смарткарти.

SSL Sockets сесията трябва да използва един от следните стандарти за SSL връзка:

SSL_RSA_WITH_RC4_128_MD5

SSL_RSA_WITH_RC4_128_SHA

SSL_RSA_WITH_3DES_EDE_CBC_SHA

Сертификатите следва да се съхраняват на смарткарти като се използва X.509 v3 стандарт. Преносът на сертификата по време на комуникационния процес е незабележим за потребителя, тъй като това се извършва, когато клиента и сървъра договарят формата.

Сертификатите ще са базирани на универсален електронен подпис, издаден от доставчик на удостоверителни услуги съгласно действащото законодателството в Р. България.

Подаваните съобщения към системата на КФН следва да са подписани с цифров подпис на източника на съобщението (публично дружество/емитента). За целта

дружеството трябва при подаване на информацията в информационния посредник да е подписало съответната форма със собствения си цифров подпис. За цифров подпис на съобщенията се използва алгоритъм SHA1 with RSA (SHA1withRSA, така както е описан в документ PKCS #1). Алгоритъмът SHA1 ще изчислява цифровото извлечение , което ще се криптира чрез RSA алгоритъм като се използва частния ключ на подписващия. Публичното дружество източник на информацията, следва да се е регистрирало предварително в КФН за подаване на информация по електронен път съгласно Правила, процедури и стандарти за организация, функциониране и управление на единната система за предоставяне на информация e-register. При регистрация на лицето в КФН се съхранява публичната част на неговия цифров сертификат с цел проверка на подаваните от него през ИА съобщения.

Публичният ключ ще се използва за декриптиране и проверка на подписа.

Ще се използва BASE64 протокол за кодиране и декодиране на цифровия подпис и за пренос на цифровия подпис през връзката. Този протокол е специфициран в RFC1521. Този RFC е част от MIME спецификациите публикувани от Internet Engineering Task Force (IETF).

За протокола описан по долу, обменяните съобщения ще са означени като затворени в кавички "съобщение".

2.3 Стартиране

Интерфейсът ще се движи от събитията възникващи при изпращане на съобщения от ИА и вътрешните операции в КФН и ще работи в реално време.

След като се направи връзката между двете системи – съгласуване на ниво SSL connections, се изпраща съобщението на клиента.

Системата на КФН се състои от сървърен процес в режим на прослушване на връзката на порт 9001.

3 Компоненти на системата

3.1 Списък на компонентите

Интерфейсът се състои от следните компоненти:

От странна на клиента / Информационен посредник/:

- Получаващ и изпращащ процес /клиент/.

От страна на КФН:

- Изпращащ и получаващ процес (Входен /Изходен сървер).

3.2 Описание на компонентите

От страна на клиента на КФН: Изпращащият процес се състои от процес, който може да инициара SSLSocket сесия към сървера на КФН на порт 9001. След успешното установяване на връзка се обменят няколко съобщения за установяване на протокола и синхронизация, след което се изпращат основните съобщения.

SSLSocket сесията ще използва стандарт TLS 1.0. Съобщенията обменяни между процеса и сървъра на КФН, трябва да са подписани с цифров подпис на клиента на ИА – публично дружество или емитент , като се използва алгоритъм SHA1 RSA. RSA алгоритъма ще използва 1024 bits ключ записан на смарткарта, която принадлежи на оторизираното лице за връзка с КФН.

Цифровият подпис ще бъде BASE64 кодиран. Стандартът BASE64 е описан в RFC1521.

От страна на КФН ще са стартирани следните компоненти: получаващ – приемащ сървър.

От страна на КФН (сървър): Контролният процес сървър директно ще комуникира с контролния процес на публично дружество или емитент. Той ще стартира SSL сесия всеки път когато има нова заявка за такава сесия. Използва се SSL стандартTLS 1.0. Съобщенията са с цифров подпис по алгоритм SHA1 with RSA и кодирани по стандарт BASE64. При установяване на SSL сесия може да се изпращат през тази сесия повече от едно съобщения.

Всички описани по горе процеси ще работят в режим - реално време.

4 Описание на процесите в интерфейса

Компонентите на интерфейса ще изпълняват следния протокол.

4.1 Протокол между клиент и системата на КФН:

Този протокол трябва да се спазва точно и стъпките да следват точният ред. Преход от една стъпка към друга извън реда посочен в този протокол ще предизвика грешка. Ако това се случи е необходимо да се затвори сесията и да се стартира отново.

Стъпка 1: КЛИЕНТ:
Отваря се нова сесия като се използва host: <ip_адрес> на машината на КФН или <DNS_име> на машината на КФН. Използва се порт 9001.

След успешно установяване на сесия и размяна на ключове, клиента изпраща до сървъра следния стринг: **"SRFSC/ext:id=<cl_system>| queueName=fsc/ext/NSInputServer"**. <cl_system> е глобалния номер на ИА присвоен от КФН.

Горното се изпълнява само при първоначалното инициализиране на сесията.

Стъпка 2: SERVER:
Сървърът отговаря :

"NAK:invalid request": Това е в случай, че синтаксисът е некоректен. Клиентът ще трябва да повтори заявката.

"NAK:service not available": Това се случва когато името cl_system е некоректно. Заявката трябва да се повтори.

"MSG_SERVER_DOWN": Това означава, че сървъра за съобщения не работи и трябва да се уведоми незабавно Администратора.

"MSG_SERVER_UP": Това е нормален отговор и означава, че комуникацията може да продължи.

Стъпка 3: CLIENT:
Клиентът трябва да повтори системната заявка "SR…" ако отговора е нещо подбно на "NAK:.." . Първо клиентът трябва да затвори сесията и след това да я отвори отново.

Клиентът трябва да уведоми КФН ако е получил съобщение "MSG_SERVER_DOWN".

Ако отговра е "MSG_SERVER_UP" клиентът трябва да изпрати следното съобщение: "MSG_INITIATE".

При успешно стартиране на новата сесия, клиентът трябва да изпрати следното съобщение: "MSG_INITIATE" през контролния канал към КФН.

Стъпка 4: SERVER:
Сървърът трябва да отговори с "MSG_ACK_INITIATE".

От тук нататък клиентът може да изпраща данни съгласно описания по-долу формат заедно със съответните цифрови подписи.

Сървърът на КФН очаква съобщенията контролния канал на порт 9001.

Стъпка 5: CLIENT:

Клиентът изпраща по контролния канал съобщение MSG_SEND_REQ.

Стъпка 6: SERVER:

Сървърът изпраща по контролния канал /порт 9001/ съобщение MSG_SEND_ACK и очаква по същия канал съобщението.

Стъпка 7: CLIENT:
Клиентът трябва да е готов да изпраща съобщения с данни .

От тази стъпка нататък сървърът и клиента комуникират като използват специфичен протокол за изпращане на съобщенията. Този протокол указва, че преди самото съобщение се изпращат четири байта информация с дължината на съобщението (виж по-долу).

Съобщението трябва да е подготвено съгласно описания по-долу формат. Цифровият подпис трябва да се пресметне за цялото съобщение като се използва SHA1 with RSA алгоритъм посредством частния ключ от смарт картата. След това подписът трябва да се кодира като се използва BASE64 алгоритъм, който променя цифровия подпис от масив от байтове в стринг от знаци. Цифровият подпис трябва да е направен с цифровия сертификат на клиента на информационния посредник и публично дружество или емитент, а не с подпис на информационния посредник.

Ако отбележим XML съобщението с SWMSG, SHA1 with RSA цифровия подпис отбележим с DS. SWMSG е низ от символи, докато DS е масив от байтове. Ако се приложи BASE64 кодиране за DS, BASE64 кодираната версия на цифровия подпис ще е също низ и ще отбележим с B64EDS.

Съобщението в крайна сметка би следвало да се състави по следния начин: "mes=<SWMSG>|sig=<B64EDS>". Преди това клиентът трябва да изпрати масив от четири байта , които означават големината на цялото съобщение /между кавичките по-горе/ в байтове (high byte first).

Клиентът очаква по канала /порт 9001/ потвърждение от сървъра на КФН за полученото съобщение.

Стъпка 8: SERVER:
Сървърът ще отговори по следните няколко начина през канала /порт 9001/:
Ако съобщението обяснено по-горе е неточно формирано (напр. Няма "mes=…" или "sig=…"), се връща съобщение "nak:invalid message format";

Ако проверката на цифровия подпис не потвърди подписа се връща съобщение “nak:different MACs”.

Ако XML съобщението е некоректно формирано, съгласно Правила, процедури и стандарти за организация, функциониране и управление на единната система за предоставяне на информация e-register на КФН се връща на клиента съобщение “nak:invalid XML message format”;

Ако XML съобщението е коректно форматирано, след запазването му в базата данни (БД) се връща отговор: ack:id=<Уникален идентификатор в БД>

Ако се случи някоя от горните грешки /съобщение nak:...../се връща съобщение “ack” към клиента, но след като се изпрати съобщението отговор за грешка.

Стъпка 9: CLIENT:
Ако клиентът получи “ack:id=<Уникален идентификатор в БД>” и запази успешно идентификатора, то трябва да върне “ack” на сървъра. При възникване на грешка в клиентското приложение, се изпраща “nak” Ако се получи съобщение от тип “nak:...” последвано от “ack” message, то клиента трябва да се опита да отстрани проблема и да изпрати съобщението отново.

Стъпка 10: SERVER:
При получаване на “ack”, сървърът завходява съобщението в деловодната система на КФН и изпраща отговор, съдържащ данни за входящ номер, дата и час на завходяване и т.н. в XML формат, според приложената XML схема.

Подава се отговор, потвърждаващ успешната регистрация на съобщението в електронния регистър на КФН и съдържащ входящия номер на документа, присвоен от документообработващата система на КФН. Отговорът е в следния формат: “mes=<RSWMSG>|sig=<B64EDS>”. Самото съобщение отговор е XML базирано и коректността му се определя от XML Schema.

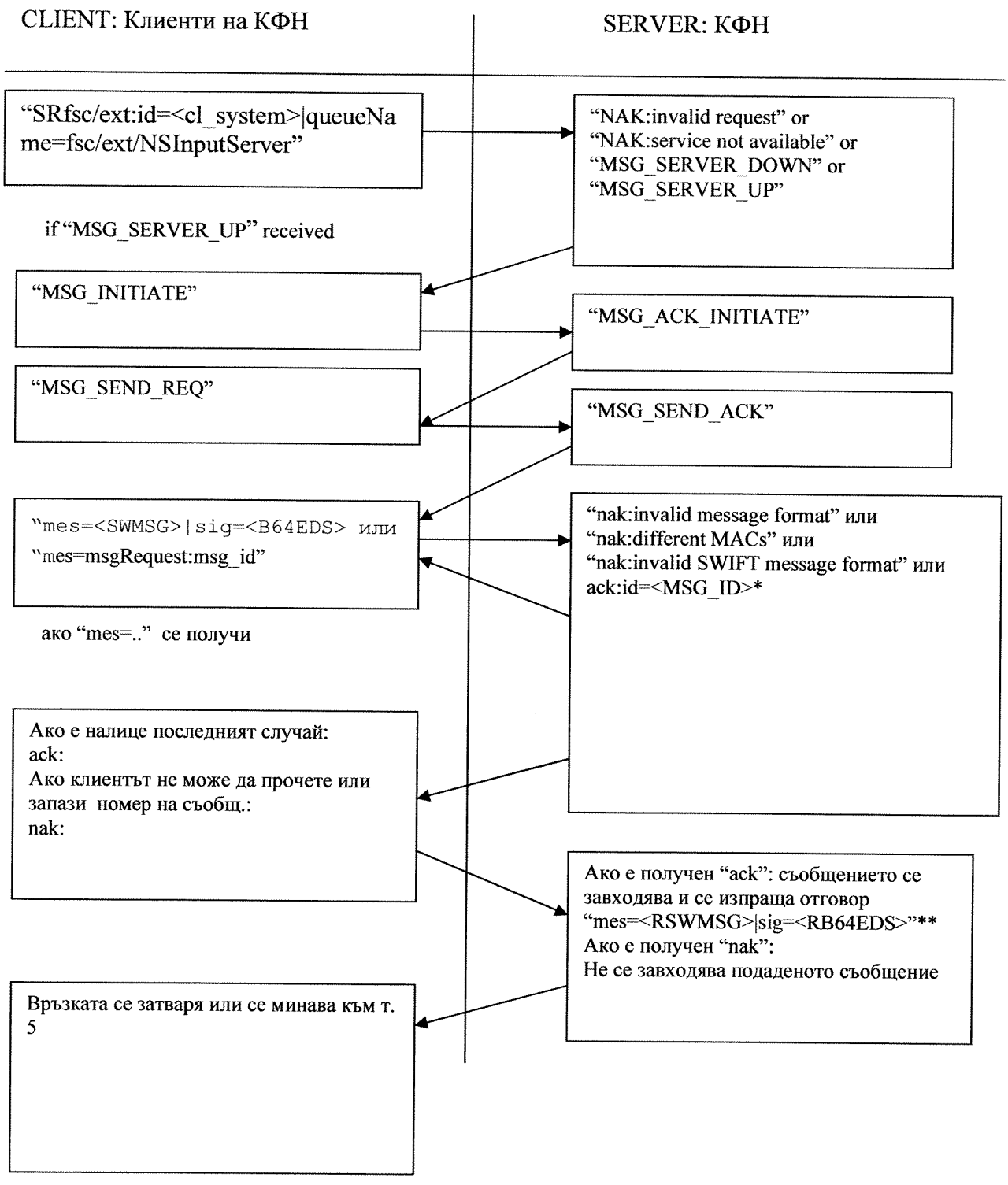
При получаване на “nak”, сървърът изтрива полученото съобщение.

В този момент, клиентът може да затвори връзката. /стъпка 11/ , ако не го направи сървърът се позиционира в изчакващ режим стъпка 5.

Клиентът може да изпрати следващото съобщение като използва по-горе описания алгоритъм – т. 5 до т.10.

Картината по долу описва потока съобщения между клиента и сървъра:

Фигура 1 – Обмен на съобщение между двете системи (клиент и КФН сървър)



* : MSG_ID ::= Id на съобщението, както е запазено в БД
** . съобщението е по схема Otgowor.xsd

Стъпка 11: CLIENT:

При закриване на връзката клиентът изпраща до сървъра по контролния канал съобщение “MSG_END_SESSION”.

Приложение 1

11	Тримесечен отчет на публично дружество и емитент на ценни книжа	Дружества със специална инвестиционна цел
12	Тримесечен отчет на банка	Дружества със специална инвестиционна цел
13	Тримесечен отчет на застрахователно дружество	Дружества със специална инвестиционна цел
15	Тримесечен консолидиран отчет на публично дружество и емитент на ценни книжа	Дружества със специална инвестиционна цел
16	Тримесечен консолидиран отчет на банка	Дружества със специална инвестиционна цел
17	Тримесечен консолидиран отчет на застрахователно дружество	Дружества със специална инвестиционна цел
18	Годишен отчет на публично дружество и емитент на ценни книжа	Дружества със специална инвестиционна цел
19	Годишен отчет на банка	Дружества със специална инвестиционна цел
20	Годишен отчет на застрахователно дружество	Дружества със специална инвестиционна цел
22	Годишен финансов отчет на дружество в производство по ликвидация или несъстоятелност	Дружества със специална инвестиционна цел
23	Годишен консолидиран отчет на публично дружество и емитент на ценни книжа	Дружества със специална инвестиционна цел
24	Годишен консолидиран отчет на банка	Дружества със специална инвестиционна цел
25	Годишен консолидиран отчет на застрахователно дружество	Дружества със специална инвестиционна цел
26	Тримесечен отчет на емитент на облигации по чл. 100е, ал. 1, т. 2, във връзка с чл. 100е, ал. 2 от ЗППЦК за спазване на задълженията на емитента към облигационерите	Дружества със специална инвестиционна цел
27	Шестмесечен отчет на емитент на облигации по чл. 100б, ал. 3 от ЗППЦК за спазване на условията по облигационния заем	Дружества със специална инвестиционна цел
28	Шестмесечен отчет на довереника на облигационерите по чл. 100ж, ал. 1, т. 2 от ЗППЦК за спазване на условията по облигационния заем	Дружества със специална инвестиционна цел
29	Представяне на покана за свикване на общо събрание на акционерите и материали за общо събрание на акционерите	Дружества със специална инвестиционна цел
30	Публикация на поканата за свикване на общо събрание на акционерите	Дружества със специална инвестиционна цел
31	Протокол от Общо събрание на акционерите	Дружества със специална инвестиционна цел
32	Уведомление за паричен дивидент	Дружества със специална инвестиционна цел
33	Уведомление за дивидент в акции (увеличение на капитала със собствени средства)	Дружества със специална инвестиционна цел
36	Откриване на производство по ликвидация	Дружества със специална инвестиционна цел
37	Несъстоятелност	Дружества със специална инвестиционна цел
40	Вътрешна информация по чл. 4 от Закона срещу пазарните злоупотреби с финансови инструменти	Дружества със специална инвестиционна цел