

Инструкция по работе с FTPS сервером Московской Биржи в тестовой среде

Оглавление

Подключение для автоматизированной загрузки отчётов	1
Адреса промышленного FTPS сервера	1
Адрес сервера FTPS в сети Интернет для тестового подключения	1
Подключение и загрузка файлов отчётов с помощью FTP-клиента	2
Расшифровка и снятие ЭЦП с полученного отчёта	4
Работа с использованием сертифицированных СКЗИ (ГОСТ криптография)	4
Работа с использованием несертифицированных СКЗИ (RSA криптография)	6

Подключение для автоматизированной загрузки отчётов

Адреса промышленного FTPS сервера

Доменное имя: ftps.moex.com

IP-адрес сервера в сети Интернет: 85.118.181.25

IP-адрес сервера для подключения через выделенную сеть: 91.203.252.70

Порт: 21, а также диапазон 49152-65534

В качестве данных аутентификации и авторизации используются имя пользователя и пароль для личного кабинета участника (ЛКУ).

Адрес сервера FTPS в сети Интернет для тестового подключения

IP-адрес тестового сервера: 91.208.232.211

Порт: 21, а также диапазон 49152-65534

Имя пользователя: ftps_for_test1

Пароль: t3E@4mYjE7

Для автоматизированной загрузки файлов отчётов используются стандартные команды протокола FTP. Потребуется установить защищённое соединение через TLS для передачи данных.

При появлении проблем с доступом к серверу обратитесь на help@moex.com

Подключение и загрузка файлов отчётов с помощью FTP-клиента

Для работы с сервером FTPS может использоваться любой FTP-клиент. Ниже на скриншотах приведён пример использования бесплатного клиента FileZilla для создания подключения и загрузки файлов с тестового сервера FTPS Московской биржи.

- 1. Запустите клиент FileZilla.
- 2. Нажмите иконку «Открыть менеджер сайтов». Откроется окно «Менеджер сайтов», где нужно заполнить данными поля для подключения к серверу, которые вы получили от службы технической поддержки.
- 3. 1 добавьте новый сайт, 2 введите имя для сайта, 3 В поле Хост введите IP-адрес. 4 — выберите способ шифрования «Требовать FTP через TLS (явный)», чтобы устанавливать защищенное соединение, 5 — укажите тип входа «Запросить пароль», чтобы обеспечить неприкосновенность пароля и не сохранять его вместе с данными о подключении, 6 укажите имя пользователя, 7 — нажмите «Соединиться».

Менеджер Сайтов	×
Выберите запись: Мои Сайты tp local To ftps MOEX pub ftp	Общие Дополнительно Настройки передачи Кодировка Хост: 3 91.208.232.211 Порт: Протокол: FTP - Протокол передачи файлов Шифрование: Требовать FTP через TLS (явный) 4 Тип входа: Запросить пароль 5 Пользователь: ftps_for_test1 6 Пароль: Цвет фона: Her Комментарии:
1 Новый Сайт Новый каталог	
Новая закладка Переименовать	
Удалить Дублировать	
	Соединиться ОК Отмена

Используется стандартный порт для создания FTPS подключения: 21. Специально заполнять поле «Порт» не требуется. Тип сервера, Режим передачи, и Кодировка могут быть определены по умолчанию.

- 4. После того, как вы нажали «Соединиться», появится поле для ввода пароля при соединении.
- 5. Далее появится запрос на сохранение ключей и паролей по вашем усмотрению.
- 6. Если появится окно «Неизвестный сертификат», установите флажок рядом с «Всегда принимать сертификат в будущих сессиях» и нажмите «ОК».

👔 Неи убе,	Неизвестный сертификат сервера. Проверьте сертификат, чтобы убедиться, что он может быть принят.						
Де	тали						
Де	иствителен с:		27.10.2022 13	:50:10			
Де	иствителен до:		28.11.2023 13	:50:09			
Ce	рийный номер	00:f9:28:40:55	:ad:23:4e:5f				
A	горитм публич	RSA c 2048 6	ит				
A	горитм подпис	и:	RSA-SHA256				
Ko	нтрольная сум	ма (SHA-256):	ce:c4:a8:88:e1 ed:7d:87:67:d	:d4:19:76:dc: c:99:98:0c:38:	20:5f:21:1f:7 46:d6:d0:13	75:f6:cd: :6b:64:ef	
Ko	онтрольная сум	ма (SHA-1):	12:af:77:a5:6f:	88:05:b6:d9:a	f:44:ef:da:b	c:98:a9:65:f3	8:53:0
Te	ма сертификата			Сертифика	т выдан		
0	бщее название:	*.beta	moex.com	Общее наз	вание:	MOEX	
A	ътернативные і	имена: *.beta.	moex.com			COM	
		beta.n	noex.com	Организац	ия:	MOEX	
				Штат или п	ровинция:	Moscow	
Де	тали сессии						
Xo	ст:	91.208.232.21	1:21				
П	оотокол:	TLS1.2					
0	бмен ключами:	ECDHE-RSA					
Ш	ифр:	AES-256-GCN	4				
M	AC:	AEAD					
При	Принять сертификат и продолжи		ить соединени	ie?			
🗌 E	🗌 Всегда принимать сертификат в будущих сессиях						
Π.	rust this certifica	d alternative h	ostnames.				

юдклі очитесь к серверу

Image: Control of the con	Файл Редактирование Вид Передача Сервер Закладки Пом	.outp			
New Torksteen Biger		A			
Control Contro <ttttt<contro< td=""> Contro<tttt<control< td=""></tttt<control<></ttttt<contro<>	Хост: Имя пользователя Па	.ролы Порт: Быстрое соединение 🔻			
Instruct diff: C/UnerWert(regret)Structure) v Instruct diff: C/UnerWert(regret) V Instruct diff: C/UnerWert(regret) V Instruct diff: C/UnerWert(regret) V </td <td>Статус: Содинение установлено, схидание приглашения Статус: Проверка сертификта Статус: Проверка сертификта Статус: Анториовались Статус: Сареце отпракило настояний ответ с неопредележным аррес Статус: Сареце отпракили пассиний ответ с неопредележным аррес Статус: Сареце отпракили пассиниий ответ с неопредележным аррес Статус: Сареце салалого УС Статус: Сареце салалого УС Статус: Сареце салалого УС</td> <td>ом. Использую существующий адрес сервера. ом. Использую существующий адрес сервера.</td> <td></td> <td></td> <td>~</td>	Статус: Содинение установлено, схидание приглашения Статус: Проверка сертификта Статус: Проверка сертификта Статус: Анториовались Статус: Сареце отпракило настояний ответ с неопредележным аррес Статус: Сареце отпракили пассиний ответ с неопредележным аррес Статус: Сареце отпракили пассиниий ответ с неопредележным аррес Статус: Сареце салалого УС Статус: Сареце салалого УС Статус: Сареце салалого УС	ом. Использую существующий адрес сервера. ом. Использую существующий адрес сервера.			~
Spations of stranger, 2612 424 64ir Parkey Tengon Spations of stranger, 2612 424 64ir	Локальный сайт: C:\Users\UserEq\repoRTS\Equities\	~	Удаленный сайт: /		~
Num dynka Passep Im dynka Passep	Equifies Examples_BACKUP Refeat Examples_BACKUP Refeat test	2	CC P. Declined_Reports EQ	4	
Examples Unica e qualita. 10.1.2022 153.016 Time e qualita. 2.644.022 153.024 XST Time e qualita. 2.644.022 153.024 2.690.028 Casama ZP-m 0.1.2.2022 154.143 10.1.2022 154.143 Time e qualita. 2.644.022 152.022.154 10.1.2022 164.144 Time e qualita. 2.644.022 152.021 154.243 10.1.2022 164.144 Time e qualita. 1.663.203 152.00 10.1.2022 164.144 Time e qualita. Time e qualita. 10.1.2022 164.144 Time e qualita. Time e qualita. 10.1.2022 164.144 Time e qualita. Time e qualita. 10.1.2022 164.144.144 Time e qualita. Time e qualita. 10.1.2022 164.144.144 Time e qualita. Time e qualita. <t< td=""><td>Имя файла</td><td>Размер Тип файла Последнее измен</td><td>Имя файла</td><td>Размер Тип файла Последнее изменение Права</td><td>Владелец/Гру</td></t<>	Имя файла	Размер Тип файла Последнее измен	Имя файла	Размер Тип файла Последнее изменение Права	Владелец/Гру
Specific Interact of the specific spec		Banna a Antia 12 01 2022 15-26-16	n 🔁 Hadabahlistan kat	0 Terreter X 16.02 2022 10:22:00	
Status Пита с файл. 21/2022 15/19:04 utfiles.ip 22/00 585 Caraza 2/00 - 01/12/2022 16/16:48 Пита с ф. 2002/2023 10/10:00 CC C004 /RU_05122022.ad 10.028 Tefornuga crun 01.12/2022 16/16:48 Пита с ф. 2002/2023 10/10:00 S фailone и 3 zaranora. Ofduură passeși: 2612 424 Gair 10.228 14/16/16:10 1 5 S фailone и 3 zaranora. Ofduură passeși: 2612 424 Gair 1 фailon x3 zaranora. Ofduură passeși: 2612 424 Gair 1 фailon x3 zaranora. Ofduură passeși: 0 Gair 5 Ceptep//Jorannu-uă фailon Hanga Фailon и 5 zaganere Passeși: 0 Gair 1	XSD	Папка с файл 26.04.2022 18:24:33	EQ	Папка с ф 20.03.2023 10:2000	
• Нябка: др 2.409 628 Счатая 20-ла 01.12.2022 18.47.37 • Ослови, RU_05722022.al 10028 Таблица стил 01.12.2022 14.16.48 • Ослови, RU_05722022.al 10028 Таблица стил 01.12.2022 14.16.48 • Ослови, RU_05722022.al 10028 Таблица стил 01.12.2022 14.16.48 • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_05722022.al • Ослови, RU_0572202.al • Ослови, RU_05722022.al • Ослови, RU_0572202.al • Ослови, RU_0572202.al • Ослови, RU_05722022.al • Ослови, RU_0572202.al • Ослови, RU_0572202.al • Ослови, RU_05722202.al • Ослови, RU_0	XSLT	Папка с файл 22.12.2022 15:19:24	cc	Папка с ф 20.03.2023 10:10:00	
	🔢 allfiles.zip	2 409 628 Сжатая ZIP-па 01.12.2022 18:47:37	Declined_Reports	Папка с ф 16.03.2023 19:22:00	
з файла в задания Наудаецинеся передачи Услешные передачи У		0002 Tabmug cruz 01.122022 141448		5	
Сервер/Локальный файл Напръ Файл на сервере Размер Приср Состояние 6 Файлы в задания Неудакцинска передачи Успешные передачи	5 файлов и 3 каталога. Общий размер: 2 612 424 байт		1 файл и 3 каталога. Общий размер: 0 байт		
Файлы в задании Неудавшиеся передачи Успешные передачи	Серкер/Логальный файл Напра Файл на серкере	Размер Приор Состояние			
	Файлы в задании Неудавшиеся передачи Успешные передачи				🔒 🕅 Эадание: пусто 🔹 🗣

1 — область ведения журнала соединения. При возникновении ошибок во время работы с FTPS соединением, вы можете обратиться на <u>help@moex.com</u> и скопировать из этой области журнальные данные.

В правой области окна (2, 3) будет отображаться структура каталогов и файлы FTPS сервера. В левой части окна (4, 5) — папки и файлы вашего рабочего места. В правой части окна выберите папку, в которую вы хотите скопировать файл отчёта. Перейдите в нужную директорию на сервере и выберите файл отчёта, затем перетащите файл с помощью мыши в выбранную папку в левой половине окна.

6 — журнал процессов передачи файлов.

Расшифровка и снятие ЭЦП с полученного отчёта

Работа с использованием сертифицированных СКЗИ (ГОСТ криптография)

На рабочем месте должен быть установлен программный комплекс АПК «Валидата Клиент» и СКЗИ "Валидата CSP": <u>http://moex.com/s1292</u>

Операции расшифрования файлов и снятия ЭЦП можно производить помощью Расширения проводника:

Для расшифрования выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню Расширения проводника пункт «Расшифровать». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа.

Этс	от компьютер 🔸 Локальный,	диск (C:) → Moscow Exchange → Reports			
^	Имя	Дата изменения	Тип	Размер	
	🔀 report_1.xml.p7s.p7e	17.03.2023 18:32	Зашифрованный	і 3 КБ	
	🔀 report_2.xml.p7s.p7e	17.03.2023 18:32	Зашифрованный	і 3 КБ	
	🔀 report_3.xml.p7s.p7e	Открыть	ррованный	і 3 КБ	
		Ореп with Sublime Text ● Переместить в OneDrive 7-Zip CRC SHA ☑ Edit with Notepad++ № Проверить на вирусы	>		
		 ПКЗИ СЭД МБ (х64) Расширение Проводника (х64) 	>	ть ЭП	
		Отправить	> 🎗 Прове	ерить ЭП	
		Вырезать Копировать	📑 Заши 🍺 Расш	фровать ифровать	
		Создать ярлык	🖓 Инфо	 рмация о файле	
		Удалить Переименовать	🖾 Показ 🎘 Выгру	ать рабочий сертификат /зить ключ	
			D		

Для того, чтобы проверить присоединённую ЭП, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню Расширения проводника пункт «Проверить и удалить ЭП»

Этот компьютер > Локальный диск (C:) > Moscow Exchange > Reports Размер Имя Дата изменения Тип Karaka and America 17.03.2023 18:32 3 KE Зашифрованный... report_2.xml.p7s.p7e 17.03.2023 18:32 3 KE Зашифрованный... 🔀 report_3.xml.p7s.p7e 17.03.2023 18:32 3 K 6 Зашифрованный... 17 03 2023 18:34 🙀 report_1.xml.p7s Полписанный фа 3 КБ Открыть report_2.xml.p7s 3 KE Open with Sublime Text k report_3.xml.p7s 3 KE 🗢 Переместить в OneDrive 7-Zip > CRC SHA > Edit with Notepad++ K 🛛 Проверить на вирусы 🖄 Отправить 🖾 ПКЗИ СЭД МБ (x64) > Расширение Проводника (х64) 💂 Создать ЭП > 🎗 Проверить ЭП Отправить > 🗙 Проверить и удалить ЭП Вырезать Зашифровать Копировать 🤂 Расшифровать Создать ярлык 🝳 Информация о файле Удалить 🖾 Показать рабочий сертификат Переименовать X Выгрузить ключ 🗁 Дополнительно > Свойства но 3 элем.: 7,29 КБ

Доступен также способ дешифрования через командную строку Windows:

- 1. Перейти в командную строку Windows: сочетание клавиш Win+R, затем в поле «Открыть» ввести cmd.
- 2. Произвести дешифрование файла с командой:

```
zpki1utl.exe -profile CLTEST1 -registry -decrypt -ldap -in
MC90000_CCX99_EQ1_16082022.p7f -out MC90000_CCX99_EQ1_16082022.p7s -recsubj
INN=009107775356
```

3. Произвести снятие электронной цифровой подписи с командой:

zpki1utl.exe -profile **CLTEST1** -registry -verify -in MC90000 CCX99 EQ1 16082022.p7s -delete 1 -out MC90000 CCX99 EQ1 16082022.xml

В указанных командах:

```
zpki1utl.exe — исполняемый файл утилиты, поставляемой с ПО «Справочник
сертификатов», располагается по умолчанию в C:\Program Files\Validata\zpki
MC90000_CCX99_EQ1_16082022.p7f — зашифрованный файл отчёта полученный с FTPS
сервера.
CLTEST1 — название профиля клиента в Справочнике сертификатов.
INN=009107775356 — указатель на сертификат специалиста Московской биржи, с
помощью которого зашифрован файл, в сетевом справочнике сертификатов.
```

Обратите внимание, что в Справочнике сертификатов должен быть подключен сетевой справочник сертификатов:

ldap://simple/vcert.pki.moex.com:50005/C=RU

Работа с использованием несертифицированных СКЗИ (RSA криптография)

На рабочем месте должен быть установлен программный комплекс "ПКЗИ СЭД МБ": <u>https://www.moex.com/s1293</u>

Операции расшифрования файлов и снятия ЭЦП можно производить помощью Расширения проводника:

Для расшифрования выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПКЗИ СЭД МБ пункт «Расшифровать». Если ранее в этом экземпляре Проводника не был загружен (или был выгружен) ключ, произойдёт загрузка ключа.



Для того, чтобы проверить присоединённую ЭП, выделите в Проводнике один или несколько файлов или каталогов и выберите в главном меню ПКЗИ СЭД МБ пункт «Проверить и удалить ЭП»

```
» Этот компьютер » Локальный диск (C:) » Moscow Exchange » Reports
```

```
^
۴
       Имя
                                               Дата изменения
                                                                      Тип
                                                                                        Размер
P
       Report_RSA_1.xml.p7a
                                                17.03.2023 19:09
                                                                      Подписанный и з...
                                                                                               4 K 6
P
       Report_RSA_2.xml.p7a
                                                17.03.2023 19:09
                                                                                               4 КБ
                                                                      Подписанный и з...
P
       Report_RSA_3.xml.p7a
                                               17.03.2023 19:09
                                                                      Полписанный и з...
                                                                                               4 K 6
                                                17 03 2023 10-11
       Report_RSA_1.xml.p7s
                                                                      Подписанный фа...
                                                                                               4 KE
P
                                  Открыть
       Report_RSA_2.xml.p7s
                                                                          писанный фа...
                                                                                               4 КБ
P
                                   Open with Sublime Text
       Report_RSA_3.xml.p7s
                                                                          писанный фа...
                                                                                               4 KБ
                               lepeмeстить в OneDrive
                                   7-Zip
                                                                       >
                                   CRC SHA
                                                                       >
                               Edit with Notepad++
Х
                               K Проверить на вирусы
                                Отправить
)
                               ПКЗИ СЭД МБ (х64)
                                                                       >
                                                                          🙎 Создать ЭП
                               Расширение Проводника (х64)
                                                                      >
                                                                           Проверить ЭП
                                                                          🗙 Проверить и удалить ЭП
                                                                      >
                                   Отправить
                                                                          🔓 Зашифровать
                                   Вырезать
                                                                          🤂 Расшифровать
                                   Копировать
                                                                          Информация о файле
ы
                                   Создать ярлык
                                                                          🖾 Показать рабочий сертификат
                                   Удалить
                                                                          X Выгрузить ключ
c
                                   Переименовать
                                                                          🗁 Дополнительно
                                                                                                                 >
                                   Свойства
рано 3 элем.: 9,45 КБ
```

Доступен также способ дешифрования через командную строку Windows:

- 1. Распаковать архив xCertUtil.zip, полученный с сайта Московской Биржи: <u>http://fs.moex.com/cdp/po/xCertUtil.zip</u>
- Перейти в командную строку Windows: сочетание клавиш Win+R, затем в поле «Открыть» ввести cmd.
- 3. Произвести дешифрование файла с командой:

```
rpki1utl.exe -profile CLTEST1 -registry -decrypt -ldap -in
MC90000_CCX99_EQ1_16082022.p7f -out MC90000_CCX99_EQ1_16082022.p7s -recsubj
INN=009107775356
```

4. Произвести снятие электронной цифровой подписи с командой:

```
rpki1utl.exe -profile CLTEST1 -registry -verify -in
MC90000_CCX99_EQ1_16082022.p7s -delete 1 -out MC90000_CCX99_EQ1_16082022.xml
```

В указанных командах:

```
rpki1utl.exe — исполняемый файл утилиты из пакета xCertUtil/pki1util.
CLTEST1 — название профиля клиента в Справочнике сертификатов.
MC90000_CCX99_EQ1_16082022.p7f — зашифрованный файл отчёта полученный с FTPS
сервера.
INN=009107775356 — указатель на сертификат специалиста Московской биржи, с
помощью которого зашифрован файл, в сетевом справочнике сертификатов.
```

Обратите внимание, что, в Справочнике сертификатов должен быть подключен сетевой справочник сертификатов:

ldap://simple/vcert.pki.moex.com:50007/C=RU