Вопросы и ответы

Прежде, чем обращаться в техническую поддержку, ознакомьтесь с этим списком вопросов и ответов. Если что-то не получается, тогда пишите нам.

Общие вопросы

1. Может ли одна лицензия использоваться на нескольких ПК?

Да, для версии Enterprise - до 10 ПК, для Ultimate - до 2 ПК, остальные версии предполагают использование одной лицензии на одном компьютере

2. Что подразумевается под "кол-во сетевых пользователей без ограничений"?

Количество сетевых пользователей, которые обращаются к зашифрованной сетевой папке. Ведь клиент может купить не одну лицензию, а скажем, 5, и тогда пользователей будет не 10, а 50. И все 50 смогут обращаться к одной сетевой папке. Это количество не ограничивается. Конечно, это теоретически, потому что количество сетевых пользователей может ограничивать сама операционная система - все зависит от лицензии операционной системы (ОС), которая установлена у клиента и от используемой ОС.

3. Нужно ли периодически продлевать лицензию?

Нет, лицензия покупается один раз. Далее пользователь не платит ни за поддержку (она бесплатна), ни за обновление программы.

4. Мне нужно установить программу на 18 ПК, сколько лицензий нужно купить?

Нужно купить две лицензии CyberSafe Enterprise

5. Можете ли сделать скидку?

Да, при покупке от 5 лицензий Enterprise мы можем сделать скидку до 15%.

6. Открыт ли исходный код программы?

Исходный код программы полностью открыт. С ним вы можете ознакомиться по адресу http://cybersafesoft.com/rus/sources/

7. Чем отличается Ultimate от Enterprise?

Сравнение различных версий программы приводится на страничке http://cybersafesoft.com/rus/products/topsecret/compare/. Основные отличия следующие:

- Поддержка КриптоПро
- Неограниченное количество сетевых пользователей
- Наличие поддержки по телефону

Но самое основное отличие в том, что Ultimate предназначена для персонального использования в некоммерческих целях. Использование Ultimate на компьютерах предприятия является нарушением лицензии. Для этого используется версия Enterprise.

8. Можно ли купить программу по безналичному расчету?

Да, можно. Обратитесь в службу поддержки.

9. Какой срок поставки программного продукта?

При оплате через Яндекс.Деньги или Avangate (для зарубежных клиентов) срок поставки - до одного часа. При оплате по безналичному расчету срок поставки зависит от того, как скоро мы увидим оплату. Если деньги поступили на счет в рабочее время, срок поставки составляет от 10 минут до одного часа.

10. Поставляется ли инсталляционный носитель?

Поставка программы происходит в электронном виде, инсталляционный носитель не поставляется. После оплаты сгенерированный лицензионный ключ будет отправлен на e-mail, указанный при оплате.

11. Помогите взломать почтовый ящик коллеги/девушки/парня/конкурента

Компания КиберСофт не оказывает услуги такого рода.

12. Мне не понравился функционал программы. Как вернуть деньги?

Увы, при такой формулировке вопроса - никак. Политика возврата средств следующая. Мы предоставляем бесплатную версию, которую можно скачать с сайта без всяких ограничений и без оплаты. Да, есть небольшие ограничение в самом функционале (количество ключей, длина ключа и т.д.), то бесплатная версия программы может полностью ознакомить с функциями программы. Если вы купили программу, не ознакомившись с ее функциями, например, вам нужно было шифрование GPT-раздела или еще что-то, то мы деньги не возвращаем.
Деньги будут возвращены только в том случае, если заявленный нами функционал у вас работает по тем или иным причинам неправильно.

13. Где можно ознакомиться с лицензией?

После установки программ лицензия доступна в файле C:\Program Files (x86)\CyberSafe Top Secret 2\license_rus.docx

Установка и переустановка программы

14. После установки программы получил сообщение "Ошибка инициализации библиотеки прозрачного шифрования"

Программу нужно переустановить. Для этого выполните следующие действия:

1. Закройте программу, удалите ее.
2. Перезагрузите компьютер
3. Установите программу и не запускайте ее.
4. Перезагрузите компьютер
5. Запустите программу

15. Не могу активировать программу после переустановки Windows/замены жесткого диска и т.д.

Чтобы после переустановки операционной системы программу можно было активировать, нужно до переустановки ее удалить при установленном соединении с Интернетом. Лицензия "вернется" в пул и вы сможете заново активировать программу. Если же возможности удалить программу не было (не было соединения с Интернетом, компьютер не запускался, забыли и т.д.), обратитесь в службу поддержки, мы вам поможем.

16. Ошибка установки контейнера корневого ГОСТ сертификата

Иногда данная ошибка возникает при использовании КриптоПРО версии 4.х. Мы рекомендуем использовать версии 3.6 и 3.9. Если необходима именно 4-ая версия, то нужно переустановить КриптоПро и программу. Последовательность буде такой:

1. Удалите КриптоПро и программу CyberSafe Top Secret, перезагрузите компьютер.
2. Установите КриптоПро версии 3.9, а затем - CyberSafe Top Secret
3. Перезагрузите компьютер и не запускайте программу
4. Обновите КриптоПро до версии 4, а программу CyberSafe Top Secret до версии 2.2.32

17. Я приобрёл у вас программу и установил на ноутбук, теперь я приобрёл себе новый компьютер и хочу перенести данную программу с ноутбука на новый компьютер. Как мне это сделать правильно?

Нужно удалить программу на старом компьютере и установить на новом. Перед удалением программы экспортируйте ваши ключи и импортируйте на новом компьютере. О том, как это сделать, написано в руководстве:

http://cybersafesoft.com/CyberSafeTopSecretUsersManual(RUS)2.pdf

Защита электронной почты

18. Интересует шифрование электронной почты. Посоветуйте, пожалуйста, продукт

Самый простой вариант - использование плагина для MS Outlook. С плагином можно ознакомиться по ссылкам:
http://cybersafesoft.com/rus/products/cybersafe-mail-encryption/
http://cybersafesoft.com/rus/blogs/cybersafe-mail/

Если у вас другой почтовый клиент, тогда можно использовать CyberSafe Top Secret для создания сертификатов
S/MIME. Главное, чтобы ваш почтовый клиент поддерживал S/MIME. О том, как настроить S/MIME-шифрование на примере
MS Outlook показано в нашей статье:
https://habrahabr.ru/company/cybersafe/blog/209642/

Обзор средств защиты почты:
https://habrahabr.ru/company/cybersafe/blog/269513/

19. Кроме стандарта S/MIME есть и другие, например, PGP. Какой из них надежнее?

Мы рекомендуем использовать стандарт S/MIME как наиболее надежный и универсальный. Наши программные продукт поддерживают только стандарт S/MIME.

20. Будет ли работать созданный в программе сертификат с моим почтовым клиентом?

Если используемый почтовый клиент поддерживает S/MIME, сертификат работать будет. За более детальными инструкциями по установке сертификата обратитесь к руководству по используемому почтовому клиенту.

21. Как настроить шифрование почты в MS Outlook?

Подробно процесс настройки шифрования в Outlook описан в нашей статье https://habrahabr.ru/company/cybersafe/blog/209642/.

22. Как настроить шифрование почты в Android?

Для этого нужно сначала установить приложения MailDroid и CryptoPlugin, поскольку стандартный почтовый клиент не поддерживает шифрование:

1. Перед настройкой шифрования в Android нужно экспортировать ваши ключи (которые вы создадите в Windows-программе CyberSafe TopSecret) и ключи всех, с кем вы планируете обмениваться корреспонденцией и загрузить на SD-карточку (или во внутреннюю память) вашего Android-устройства.
2. Проверяем настройки программы MailDroid. Откройте экран настроек. Перейдите в раздел Encryption Plugin. Убедитесь, что выбран режим шифрования S/MIME и включен переключатель Allow MailDroid to decide.
3. Откройте Crypto Plugin. Перейдите на вкладку S/MIME и выберите команду Import Certificate.
4. Первым делом нужно импортировать корневой сертификат. Его файл называется Root Certificate
5. Выберите файловый менеджер, который вам удобно использовать, чтобы указать путь к сертификату. Далее нужно перейти к каталогу, в который вы поместили выбрать Root Certificate.cer. Программа спросит, как открыть файл. Нужно выбрать "Стандартный".
6. Импортированный сертификат появится в списке сертификатов. Далее операцию импорта нужно повторить для вашего личного сертификата (.pfx) и сертификатов всех, с кем вы планируете обмениваться зашифрованными сообщениями и ЭЦП. При импорте личного сертификата будет запрошен пароль. Обратите внимание: ваш личный сертификат помечен в списке как PRIVATE.
7. После импорта сертификатов можно приступить к обмену зашифрованными/подписанными сообщениями.

8. При создании нового сообщения в MailDroid вы можете подписать и зашифровать его. Для этого, если нужно только подписать включите переключатель Sign. Если нужно не только подписать, но и зашифровать сообщение, тогда включите еще и переключатель Encrypt. При подписании сообщения нужно выбрать, какой сертификат будет использоваться. Выбор сертификата происходит в области SIGNERS. Скорее всего, у вас будет всего один сертификат.

23. Интересует срок действия ключа - как вы рекомендуете - устанавливать небольшой срок действия и чаще менять ключ или установить продолжительный срок (5 лет или больше)?

Все зависит от поставленных задач. Если требуется длительная защита почтового ящика, то выбирайте срок 5-10 лет. Дело в том, что если выйдет срок действия ключа, то расшифровать сообщения ним вы сможете, а вот зашифровать - уже нет. Представьте такую ситуацию. Вы сгенерировали сертификат сроком действия 365 дней (1 год). Вы ведете переписку с коллегами по работе. Переписка зашифрована и все хорошо. Прошел год. Зашифровать новые сообщения вы не можете, так как срок действия сертификата истек. Вы генерируете новый сертификат, обмениваетесь ним с коллегами. В результате получится, что вы сможете создать/зашифровать новые сообщения, но не сможете расшифровать старые, написанные вам год назад - ведь для их шифрования использовался ваш старый сертификат.

Если переписка потеряет свою актуальность через год, тогда ничего страшного. Но бывают моменты, когда нужно отыскать какое-то старое письмо, с какими-то важными документами, в этом случае лучше увеличить срок действия сертификата, скажем до 5 лет. Вместо того чтобы часто менять сертификаты, лучше установите длину ключа в 4096 или даже 8192 бит (последняя рекомендуется только на мощных компьютерах) и используйте сложный пароль, содержащий буквы, цифры и неалфавитные символы.

24. Есть ли плагин шифрования для Mozilla Thunderbird?

К сожалению, плагина для Mozilla у нас нет.

Шифрование файлов для передачи

25. Не получается зашифровать файлы, пытаюсь использовать шифрование для передачи, но размер создаваемого архива меньше, чем размер файлов. Распаковать архив тоже не получается.

В старых версиях программы размер создаваемого архива был ограничен и об этом было сказано в руководстве. Цель ограничения - практически все SMTP-серверы не позволяют пересылать большие файлы. В версии 2.2.32 это ограничение было снято. Если вам нужно использовать функцию "Шифрование для передачи" для шифрования больших объемов информации, установите последнюю (2.2.32 на момент написания этих строк) версию программы. Ее можно скачать с сайта.

26. Процесс шифрования идет медленно

Скорость процесса шифрования зависит от выбранных параметров шифрования, производительности процессора и дискового накопителя. Существенно ускорить процесс можно двумя способами: модернизировать компьютер (более мощный процессор, SSD-накопитель) или уменьшив размер ключа.

Прозрачное шифрование. Шифрование сетевых папок

27. Не получается зашифровать сетевую папку. Файлы в ней незашифрованы, хотя папка включена

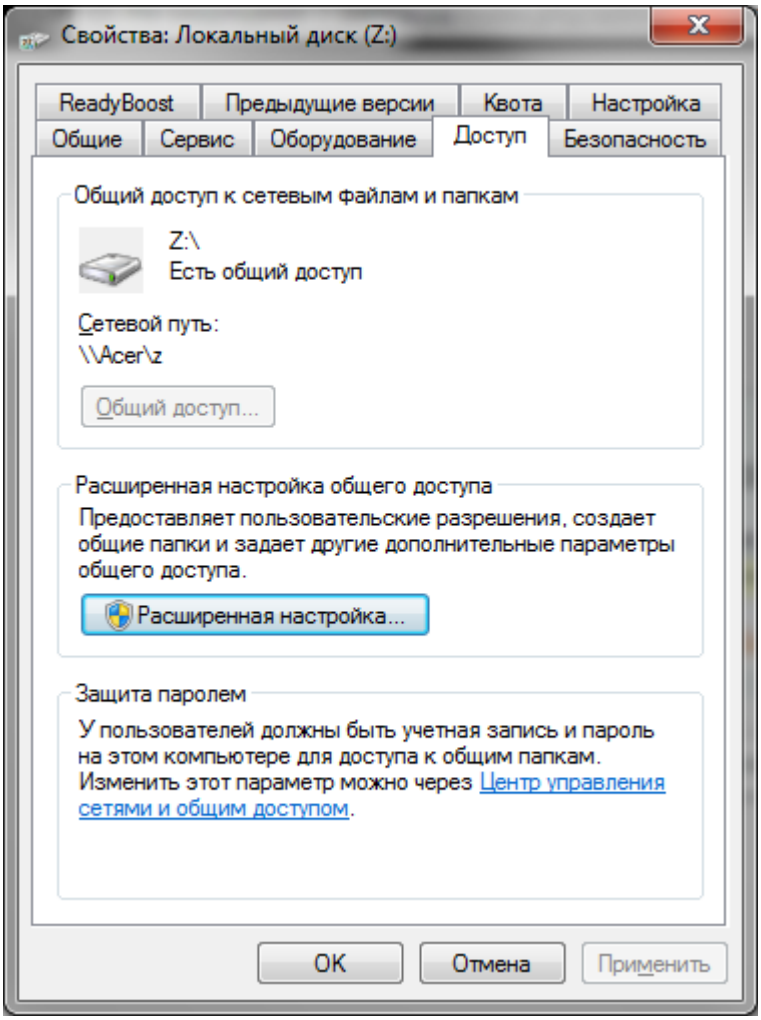
Особенность драйвера прозрачного шифрования такова, что драйвер не должен быть установлен на компьютере, на котором физически находится шифруемая сетевая папка. Другими словами, программа CyberSafe Top Secret не должна устанавливаться сервере (или компьютере, который выступает в роли сервера, предоставляя общие сетевые папки).

28. Можно ли расшарить зашифрованную папку, если есть только два компьютера?

В ответе на вопрос 26 было сказано, что на сервер, то есть компьютер, на котором физически размещена зашифрованная папка, нельзя устанавливать CyberSafe Top Secret, если планируется совместное использование зашифрованной папки. Данная схема подразумевает наличие как минимум трех компьютеров: "сервер" и два клиента.

Но что если есть только два компьютера? В этом случае можно использовать общий доступ к виртуальному диску - создайте виртуальный диск и предоставьте к нему общий доступ.

Нажмите кнопку Расширенная настройка и в появившемся окне включите общий доступ. Должно получиться так



Далее нужно настроить права доступа:

1. В окне свойств диска нажмите кнопку Расширенные настройки
2. В открывшемся окне нажмите кнопку Разрешения
3. Выберите группу Все, установите все флажки под колонкой Разрешить, как показано на скриншоте

29. Как правильно выполнить резервное копирование зашифрованной папки?

Программа, выполняющая резервное копирование, должна поддерживать сохранение файловых потоков (Acronis, WinRAR). Подробнее можно прочитать по ссылке: https://habrahabr.ru/company/cybersafe/blog/259323/

30. При создании резервной копии файловые потоки не были скопированы. Может быть, есть способы добавить недостающие потоки?

К сожалению способа добавить недостающие файловые потоки нет, если они изначально не были скопированы программой. Следовательно, расшифровать файлы не получится.

31. Необходимо автоматически включать папку при прозрачном шифровании в момент запуска ПК. В настройках и документации подобной функции нет, как это сделать? Практическое применение: резервное копирование в облако (не синхронизация, именно односторонний бэкап). Для чего создал папку с прозрачным шифрованием и планирую настроить туда копирование по расписанию некой информации. Каждый раз при включении ПК заходить и включать папку, вводя пароль, крайне неудобно.

Такой возможности у нас, к сожалению нет. Но вы можете попробовать использовать альфа-версию приложения Шифрование дисков:
http://cybersafesoft.com/rus/products/disk-encryption/

В ней есть функция автоматического монтирование крипто-диска. Далее, используя дельта-синхронизацию крипто-контейнера, можно копировать в облако не весь файл крипто-диска, а только тех его частей, которые изменились. Подробно о дельта-синхронизации написано в нашей статье:
https://habrahabr.ru/company/cybersafe/blog/280792/

32. В чем основные преимущества прозрачного шифрования CyberSafe TopSecret по сравнению с EFS?

Основные недостатки EFS - невозможность сетевого шифрования (если оно вам нужно, то необходимо использовать другие протоколы шифрования данных, например, IPSec) и

отсутствие поддержки других файловых систем. Если вы скопируете зашифрованный файл на файловую систему, которая не поддерживает шифрование, например, на FAT/FAT32, файл будет дешифрован и его можно будет просмотреть всем желающим. Ничего удивительного в этом нет, EFS — всего лишь надстройка над NTFS.

Что же касается прозрачного шифрования CSTS, то поддерживается сетевое шифрование, при этом данные по сети передаются в зашифрованном виде, а при копировании на носитель при выключенной папке прозрачного шифрования вы получите зашифрованные файлы, которые, если не были скопированы файловые потоки, и расшифровать то будет невозможно.

Подробнее можно прочитать здесь: https://habrahabr.ru/company/cybersafe/blog/251041/

33. Все администраторы домена получают доступ к данным вопреки желаниям владельца данных. Имеется ли возможность ограничить права администраторов домена средствами самой программы?

Программа не ограничивает права администраторов домена. Попробуйте выполнить ограничение средствами операционной системы. Желаемого эффекта можно добиться, если не добавить к папке ключ администратора, тогда он не сможет расшифровать файлы, но получит к ним доступ. Файлы будут зашифрованы и администратор не сможет их прочитать. Поэтому частично задача разграничения доступа будет решена.

Шифрование дисков. Виртуальные диски

34. После монтирования виртуальный диск оказался пуст, хотя вчера все было нормально. Что делать?

Чаще всего подобная ситуация может произойти из-за физического повреждения данных на жестком диске. Рекомендуем проверить ваш жесткий диск на наличие плохих секторов.

Для восстановления данных можно использовать любую программу восстановления, например, R-Studio (http://www.r-studio.com/ru/)

Приказом Министерства юстиции РФ от 26 ноября 2015 г. № 269, R-STUDIO была включена в список требований к минимальной комплектации материально-технической базы по

нескольким видам судебных экспертиз проводимых в федеральных бюджетных судебно-экспертных учреждениях Министерства юстиции Российской Федерации.

Подмонтируйте диск и произведите восстановление данных. Подробная инструкция: http://cybersafesoft.com/r-studio.pdf

35. Есть ли возможность автоматического монтирования виртуальных дисков?

В программе CyberSafe такой возможности, к сожалению, нет. Но она есть в другой нашей разработке - в программе Шифрование дисков, доступной по ссылке: http://cybersafesoft.com/rus/products/disk-encryption/

36. В облако помещен крипто-диск. Как сделать так, чтобы он синхронизировался не полностью, а только измененные части?

Для этого нужно использовать дельта-синхронизацию. Подробнее данный процесс описан в нашей статье http://cybersafesoft.com/rus/blogs/delta-sync/

37. Поддерживается ли GPT?

К сожалению, GPT не поддерживается и зашифровать GPT-диски нашей программой не получится.

38. После шифрование диск исчез из системы как на обучающих видео, но он не активен для монтажа как на видео. Активна только одна кнопка Восстановить, после ее нажатия диск доступен для монтажа, но при этом Windows до момента монтажа видит этот диск как RAW и предлагает всегда его отформатировать, то есть одно неловкое движение руки и можно случайно стереть данную зашифрованную область со всей информацией.

Сначала нужно нажать кнопку Восстан., появится окошко Windows, в нем нужно нажать кнопку Отмена. После этого нужно вернуться в окно программы и нажать кнопку Монтировать. Об этом написано в руководстве пользователя (процесс шифрования диска описан, начиная со страницы 121):

http://cybersafesoft.com/CyberSafeTopSecretUsersManual(RUS)2.pdf

39. Программа не поддерживает шифрование больших объемов данных

Если речь идет о модуле Шифровать файлы, Шифрование для передачи, то, действительно, есть ограничение на размер файла - 270 Мб. Ограничение связано с тем, что большинство SMTP-серверов не позволяют передавать большие файлы, поэтому мы рекомендуем не использовать функцию шифрования файлов для файлов, размер которых превышает 100 Мб, об этом сказано на странице 79 Руководства программы. Данное ограничение было снято в версии 2.2.32, поэтому можно установить ее и использовать модуль Шифрование для передачи без ограничений.

Однако для шифрования больших объемов данных и для более удобной работы с ними рекомендуется создать криптоконтейнер (Шифрование дисков, Виртуальный диск) и поместить в него все необходимые файлы. Файл виртуального контейнера можно передать любым удобным образом, например, опубликовать в облаке, разместить на FTP-сервере, сетевом диске и т.д. Программа не накладывает каких-либо ограничений на размер этого файла и на размер файлов, находящихся внутри контейнера.

40. Я неоднократно замечал, что случайным для меня образом виртуальный диск и зашифрованная папка остаются доступными после перезагрузки или выключения/включения ПК

Очевидно, речь идет не о полном выключении, а о режиме гибернации. По умолчанию в современных версиях Windows включен режим быстрого запуска - при выключении питания системные службы не останавливаются, а происходит их гибернация. Соответственно, при следующем запуске компьютера виртуальный диск и зашифрованная папка оказываются смонтированными. Эту особенность нужно учитывать: вы можете или отключить режим гибернации в Windows или размонтировать виртуальный диск и отключать зашифрованную папку перед завершением работы.

41. Проблема Can't unmount the host device при попытке зашифровать раздел

Раздел, который вы хотите зашифровать, используется какой-то программой. Завершите работу этой программы и повторите процесс шифрования

42. С помощью вашей программы я создал криптоконтейнер (размером чуть меньше 2 ГБ) и зашифровал его. Папка с криптоконтейнером в сетевом доступе. При попытке его открыть с другого компьютера (на котором тоже установлена программа) происходит ошибка Error mount volume: failed with error 00000002.

Мы не гарантируем корректной работы виртуального диска по сети - это так называемый побочный эффект - в большинстве случаев виртуальный диск можно "расшарить", но в некоторых случаях - нет. Как правило, ошибки при работе с расшаренным виртуальным диском происходят из-за неправильных прав доступа. Если настроить права доступа не получается (см. вопрос 27), тогда можно использовать программу Шифрование дисков, которая доступна по ссылке: http://cybersafesoft.com/rus/products/disk-encryption/

43. Решил создать зашифрованный раздел диска как в видео https://www.youtube.com/watch?v=EBrbJX_UDpQ, после создания зашифрованного раздела, раздел скрывается, но кнопка "монтировать" не активна, только "восстановление" доступна, после нажатия этой кнопки, раздел появляется, и тогда кнопка "монтировать" становится активной, но раздел не скрыт и постоянно просит его отформатировать, как эту проблему исправить?

После того, как диск будет зашифрован, вы увидите его состояние — зашифрован, скрытый. Это означает, что ваш диск был зашифрован и скрыт — он не будет отображаться в Проводнике и других высокоуровневых файловых менеджерах, но его будут видеть программы для работы с таблицей разделов.

Обратите внимание, что в оснастке Управление дисками зашифрованный раздел отображается как раздел с файловой системой RAW, то есть без файловой системы вообще. Это нормальное явление — после шифрования раздела Windows не может определить его тип. Именно поэтому, когда вы нажмете кнопку Восстан., чтобы сделать диск видимым, Windows предложит его отформатировать.

Этого нельзя ни в коем случае делать, поскольку вы потеряете все данные. Именно поэтому программа скрывает зашифрованные диски — ведь если за компьютером работаете не только вы, другой пользователь может отформатировать якобы не читаемый раздел диска.

Для того чтобы монтировать том, выделите его в Рабочей области, нажмете Монтировать в Панели опций и в открывшемся окне выберите свободную букву, на которую будет смонтирован созданный том в качестве логического диска операционной системы.
Другими словами, сначала нужно нажать кнопку Восстан., а потом - кнопку Монтировать.
Подробная информация приводится в руководстве программы, начиная со страницы 121:

http://cybersafesoft.com/CyberSafeTopSecretUsersManual(RUS)2.pdf

44. Как повлияет отключение света на смонтированные папки, диск, токен (т.е не будут демонтированы должным образом из программы)?

При отключении света диски не размонтируются должным образом. Рекомендуем использовать источник бесперебойного питания.

45. Как реализовать доступ к своим файлам в облаке с чужого компьютера (при наличии токена)?

Добавить сертификат пользователя к уже имеющимся в настройке облачной папки, и разослать его открытый ключ всем участникам шифрования облачной папки.