Инфраструктура открытых ключей

Подготовили

Байраш Анита,

Захарова Виктория,

Сокол Мария

# 1. Архитектура приложения

В системе присутствует доверенный центр CA, сервер S, хранящий открытый справочник сертификатов с их статусами, сервер C3, хранящий ресурсы - документы, и клиенты: С1 и С2.

# 2. Технологии, методы и алгоритмы

Данное приложение написано на языке Java с использованием библиотеки Swing для создания графического интерфейса. Передача данных между компонентами системы осуществляется с помощью сокетов.

Сертификаты хранятся на S в репозитории Java KeyStore, созданном специально для этих целей.

CA хранит свой самоподписанный сертификат и закрытый ключ тоже в своем KeyStore под паролем, который вводится с консоли администратором при запуске CA (для доступа к сертификату нужно знать alias - имя ячейки, где он хранится (можно назвать это паролем сертификата), для доступа к ключу - пароль для этого ключа, для доступа к самому хранилищу также вводится соответствующий пароль). Но в реальной жизни его закрытый ключ, конечно, хранится в невероятно защищенном месте.

S также хранит в своем репозитории под паролями пару своих ключей, в реальности, опять же, хорошо защищенных. Они понадобятся ему для подписи своих ответов клиентам. Открытый ключ S при его запуске передается СА, чтобы тот потом передавал его клиентам.

Асимметричное шифрование - RSA, симметричное (в частности, при шифровании документов) - AES. Разделение секрета - схема Шамира.

# 3. Взаимодействие компонент системы

## 3.1. Сертификация

Клиенты могут в любой момент получать/обновлять сертификат у СА (равно как и использовать текущий сертификат, если в новом на данный момент нет необходимости). При получении сертификата они посылают СА данные о себе, своей организации, адресе и т.п. СА может отклонить или принять их запрос. В последнем случае он генерирует пару ключей и дает клиенту флешку, где хранится его открытый ключ, сертификат клиента, закрытый ключ клиента и подписанное закрытым ключом СА имя клиента. Флешка особенная, подпись на ней защищена от копирования и удаления. Клиент проверяет ее, когда считывает сертификат, чтобы убедиться, что выбранный носитель действительно получен от СА и предназначен клиенту. Сервер С3 использует ту же процедуру получения сертификата, что и C1 и С2, и так же имеет выбор, просить новый сертификат или использовать свой текущий сертификат, если в новом на данный момент нет необходимости (но, в отличие от клиентов, только при запуске, а не в любой момент, так как считается, что сервер работает долгое время).

## 3.2. Авторизация

С1, С2 и С3 используют одну и ту же процедуру взаимной авторизации, а именно:

1) Первый пользователь отправляет второму свой сертификат, подписанный своим закрытым ключом.

2) Второй пользователь извлекает из сертификата открытый ключ и с его помощью проверяет подпись присланного сообщения. При успешной проверке второй пользователь проверяет подпись сертификата, используя открытый ключ СА. Если проверка прошла успешно, он обращается к S для проверки статуса сертификата. При этом проверяется подпись S. Если она верна и сертификат активен, аутентификация первого пользователя считается завершенной успешно.

3) При успешной аутентификации первого пользователя то же происходит в обратную сторону. В итоге оба пользователя знают открытые ключи друг друга, получая возможность обмениваться данными в зашифрованном виде.

Клиент после запуска может подключиться к любому клиенту или хранилищу документов, при этом сразу после подключения будет проведена взаимная авторизация.

## 3.3. Получение документов

С3 хранит для каждого документа пользователя или список пользователей, имеющих к нему доступ. Право на доступ к документу проверяется при каждом запросе на этот документ.

Документы передаются в зашифрованном виде, а также подписываются C3.

Перед прочтением файла клиенты проверяют подпись, чтобы убедиться, что файл получен от С3, и в случае успешной проверки обращаются к S, чтобы проверить, не оказался ли к этому времени сертификат С3 отозван. При получении ответа от S проверяется его подпись. Если все в порядке, расшифровывают документ своим закрытым ключом.

При необходимости согласованного доступа к документу нескольких лиц для этого документа на С3 генерируется секрет. Им документ шифруется, затем секрет разбивается, части высылаются клиентам, а сам секрет уничтожается.

При запросе одного из совладельцев такого документа на его получение С3 посылает остальным совладельцам запросы на получение частей секрета. После получения необходимого количества этих частей (в нашем случае 2) секрет восстанавливается, им расшифровывается документ, затем секрет удаляется. Каждый совладелец имеет право согласиться или отказаться от предоставления C3 своей части ключа. Документ высылается просившему клиенту, причем этот документ зашифрован его открытым ключом и, как и при любом обмене данными между клиентами, подписан отправителем.

# 4. Руководство пользователя

## 4.1. Запуск СА

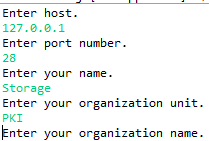
Первое, что вам нужно запустить - СА. При этом нужно будет ввести с консоли два пароля: для доступа к хранилищу СА и для доступа к его закрытому ключу. В реальной жизни пароли сложные, но вы оба раза введите "capassword".

## 4.2. Запуск Storage

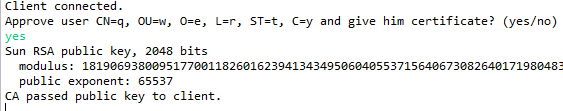
Хранилище сертификатов - следующая компонента системы, которую необходимо запустить. Оно также попросит у вас пароль для своего key storage и для своего закрытого ключа. В реальной жизни, опять же, эти пароли уникальные, сложные, но вам опять повезло: введите оба раза "storagepassword".

## 4.3. Запуск C3 (Resource Storage)

Следующий шаг - запуск хранилища документов. Здесь паролей вам вводить не придется, но нужно будет ввести хост (вводите 127.0.0.1) и порт (вводите 28) компьютера, а затем имя, организацию и другие идентифицирующие вас данные, а также место хранения вашего сертификата, то есть путь к флешке. Далее вас спросят, желаете ли вы использовать существующий сертификат или получить новый. Если вы запускаете С3 в первый раз, просите новый.

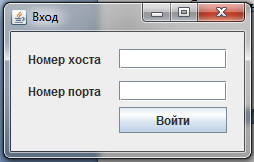


При всяком запросе сертификата СА будет спрашивать, одобрить ли пользователя с такими-то данными, выдавать ли ему сертификат. Почувствуйте себя администратором не только хранилища документов, но и вездесущим администратором CA по совместительству, ответьте положительно. Это должно выглядеть так:

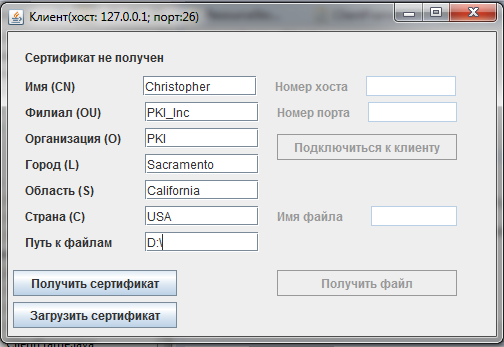


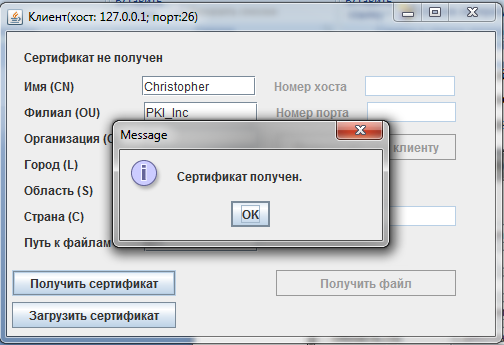
## 4.4. Запуск C1

Запустите класс Authorization и введите хост (127.0.0.1) и порт (26).



Заполните анкету и укажите путь к флешке. Если сертификат у вас уже есть, вы можете загрузить его, не обращаясь к СА. Если нет или если вы хотите новый, попросите новый. При этом не забудьте перевоплотиться на секунду снова в администратора СА и разрешить выдачу сертификата.





## 4.5. Запуск С2

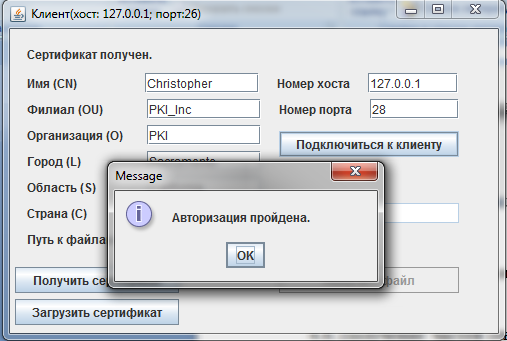
Еще раз запустите Authorization повторите предыдущие шаги (но с портом 27).

## 4.6. Получение частей секрета

Если вы хотите иметь возможность в будущем читать документ номер 3, вернитесь в окно Resource Storage и введите 1 (будут высланы части секрета), иначе - 0.

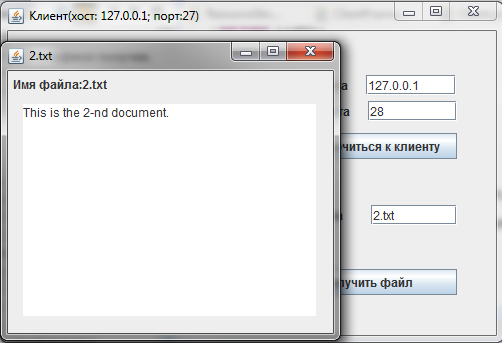
## 4.7. Подключение клиентов к C3

Если вы желаете получать документы от С3, ведите его хост и порт, далее должна произойти процедура взаимной авторизации:

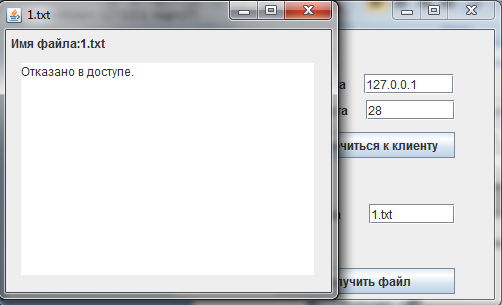


## 4.8. Получение документов

С1 имеет доступ к 1.txt, C2 - к 2.txt.



При запросе не своего документа вы увидите сообщение:



Для доступа к 3.txt другой клиент должен ввести "yes", выражая этим свое согласие выслать С3 свою долю ключа:

