А. О. Меньшенин, М. С. Панфилова

СИСТЕМА СТРОГОЙ АУТЕНТИФИКАЦИИ НА БАЗЕ ОДНОРАЗОВЫХ ПАРОЛЕЙ С ИСПОЛЬЗОВАНИЕМ ИНФРАСТРУКТУРЫ ОПЕРАТОРА МОБИЛЬНОЙ СВЯЗИ

В последнее время в России существенно возрос интерес к электронным сервисам. Услуги, предоставляемые этими сервисами, могут носить различный характер и иметь разную степень важности: получение общей информации, осуществление платежей, использование различных приложений, подача отчетов, предоставление государственных услуг и др. Пропорционально с ростом частоты и значимости таких онлайн-транзакций увеличиваются и связанные с ними риски. Одной из наиболее критичных проблем является гарантированное определение участников транзакции, т. е. аутентификация пользователей. Возможный путь решения этой проблемы — создание системы аутентификации, призванной обеспечить доверенное электронное пространство, в рамках которого участники могли бы легко и безопасно осуществлять различные удаленные операции.

Среди технических средств, используемых для осуществления аутентификации при электронном взаимодействии, одним из наиболее эффективных и гибких является использование одноразовых паролей (One-Time Password — OTP) [1]. На сегодняшний день одноразовые пароли уже получили широкое распространение как надежное и удобное средство аутентификации. Одноразовый пароль обычно представляет собой сгенерированную последовательность символов (так называемый токенкод), которая периодически меняется и имеет ограниченное «время жизни», т. е. по прошествии некоторого временного отрезка, когда комбинация сменится, предыдущая будет уже непригодна для аутентификации. При этом алгоритм генерирования токенкода синхронизован с сервером таким образом, что для проверки подлинности предъявленного кода проверяющей стороне не нужна никакая дополнительная информация. Принцип работы такого токена основан на вычислении односторонней функции от некоторого секретного значения (начального вектора генерации) и счетчика генераций, в качестве которого может использоваться текущее время [2]. Технически генераторы одноразовых паролей могут быть выполнены в различных форм-факторах — как аппаратных, так и реализованных программно. Большинство реализаций, однако, имеют существенные недостатки. Специализированные аппаратные токены достаточно дороги и невыгодны для массового использования, а программные (в частности, мидлеты для мобильных телефонов) обладают невысоким уровнем безопасности. Таким образом, ясно очерчивается потребность в реализации генератора одноразовых паролей (и системы аутентификации в целом), удовлетворяющего следующим оценочным критериям:

- легкость использования;
- безопасность используемых алгоритмов и протоколов;
- гибкость реализации;
- экономичность аппаратной реализации.

К вышеперечисленному стоит прибавить также потребность пользователя иметь генератор «под рукой» в любой момент.

Обозначенные требования достаточно эффективно могут быть удовлетворены при использовании ресурсов оператора мобильной связи.

В результате проведенного анализа авторы пришли к двум альтернативным вариантам реализации генератора одноразовых паролей (токена) с использованием ресурсов оператора мобильной связи: серверному и клиентскому.

Первый вариант подразумевает использование виртуального токена, расположенного на сервере. При данном подходе вся криптографическая информация (начальный вектор генерации,

текущее значение счетчика) хранится на сервере под защитой специализированного аппаратного модуля безопасности (АМБ), токенкод генерируется внутри защищенного периметра АМБ по запросу пользователя и передается ему посредством SMS-сообщения. Схематично процесс аутентификации пользователя изображен на рис. 1.

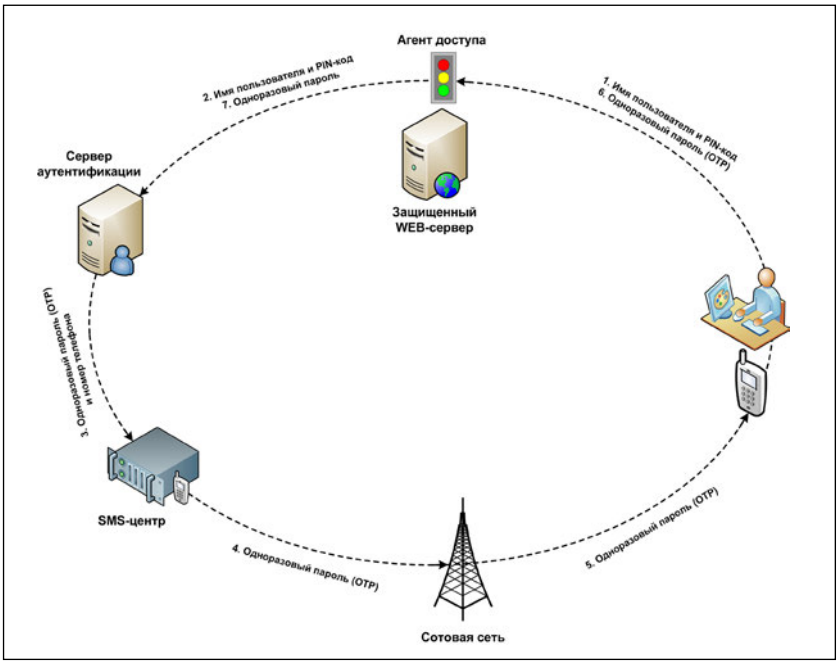

Рис. 1. Процесс аутентификации пользователя при использовании виртуального токена, располагающегося на сервере

При входе на защищаемый ресурс (например, WEB-портал) пользователь вводит имя и пароль (PIN-код). На основании имени пользователя сервис аутентификации определяет номер телефона, соответствующий этому имени, и пересылает на него токенкод в виде SMS-сообщения. Пользователь вводит полученный на свой телефон токенкод и получает доступ к требуемому ресурсу.

В указанной схеме токенкод генерируется на основе текущего времени и имеет ограниченную продолжительность действия.

К преимуществам такой схемы аутентификации следует отнести простоту ее внедрения: она не нуждается в специальной интеграции в инфраструктуру оператора связи, для аутентификации клиенту не требуется никакого дополнительного программного обеспечения или оборудования. В качестве основного недостатка необходимо отметить передачу токенкода в открытом виде посредством SMS-сообщения. Влияние данного фактора, однако, может быть ограничено периодом действия токенкода.

Второй вариант подразумевает размещение генератора одноразовых паролей непосредственно на SIM-карте абонента. SIM-карта в телефоне может рассматриваться как специализированное криптографическое устройство (смарт-карта), полностью интегрированное со считывателем и дисплеем в комбинации с сетевыми функциями. Генератор реализуется в виде специального приложения (SIM-апплета), размещаемого в отдельном домене безопасности (SecurityDomain) SIM-карты [3]. Там же располагается вся необходимая для генерации криптографическая информация. Таким образом, все критические операции выполняются внутри защищенного периметра SIM-карты, а наружу выдается только сгенерированный токенкод. Соответствующий процесс аутентификации изображен на рис. 2.

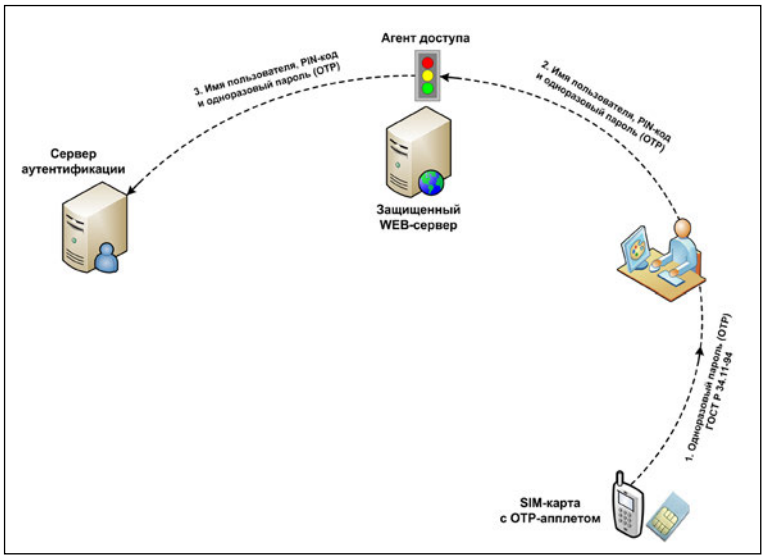

Рис. 2. Процесс аутентификации пользователя при использовании токена, располагающегося на SIM-карте абонента

При входе на защищаемый ресурс (например, WEB-портал) пользователь вводит имя и пароль, после этого система запрашивает одноразовый код доступа. Апплет для генерации токенкода размещается на SIM-карте мобильного телефона. Пользователь вызывает приложение из меню SIM-карты, вводит сгенерированный токенкод и получает доступ к требуемому ресурсу.

В представленной схеме аутентификации токенкод генерируется на основе текущего значения счетчика генераций и не имеет временных ограничений, т. е. допускает отложенное использование.

Основное преимущество данного подхода — обеспечение повышенного уровня безопасности. Однако для его успешной реализации требуется решение двух задач:

- ресинхронизации счетчиков на сервере и клиенте;
- интеграции решения в инфраструктуру оператора связи.

Задача ресинхронизации счетчиков обусловлена тем, что счетчики на клиентской и серверной сторонах работают независимо друг от друга: счетчик на клиенте увеличивается в момент генерации очередного токенкода, а счетчик на стороне сервера — только после удачной его проверки. Таким образом, возможны ситуации, в которых пользователь по каким-либо причинам не использовал сгенерированный одноразовый пароль и счетчик на клиентской стороне «убежал» вперед. Возможным решением проблемы является использование так называемого «окна», когда сервер сравнивает значение токенкодов не только для текущего счетчика, но и для некоторого предопределенного количества последующих, выбирая из них подходящее и корректируя счетчик на своей стороне.

Задача интеграции предложенного решения в инфраструктуру оператора связи представляет собой весьма трудоемкий процесс. Рассмотрим его на примере некоторого абстрактного оператора (см. рис. 3).

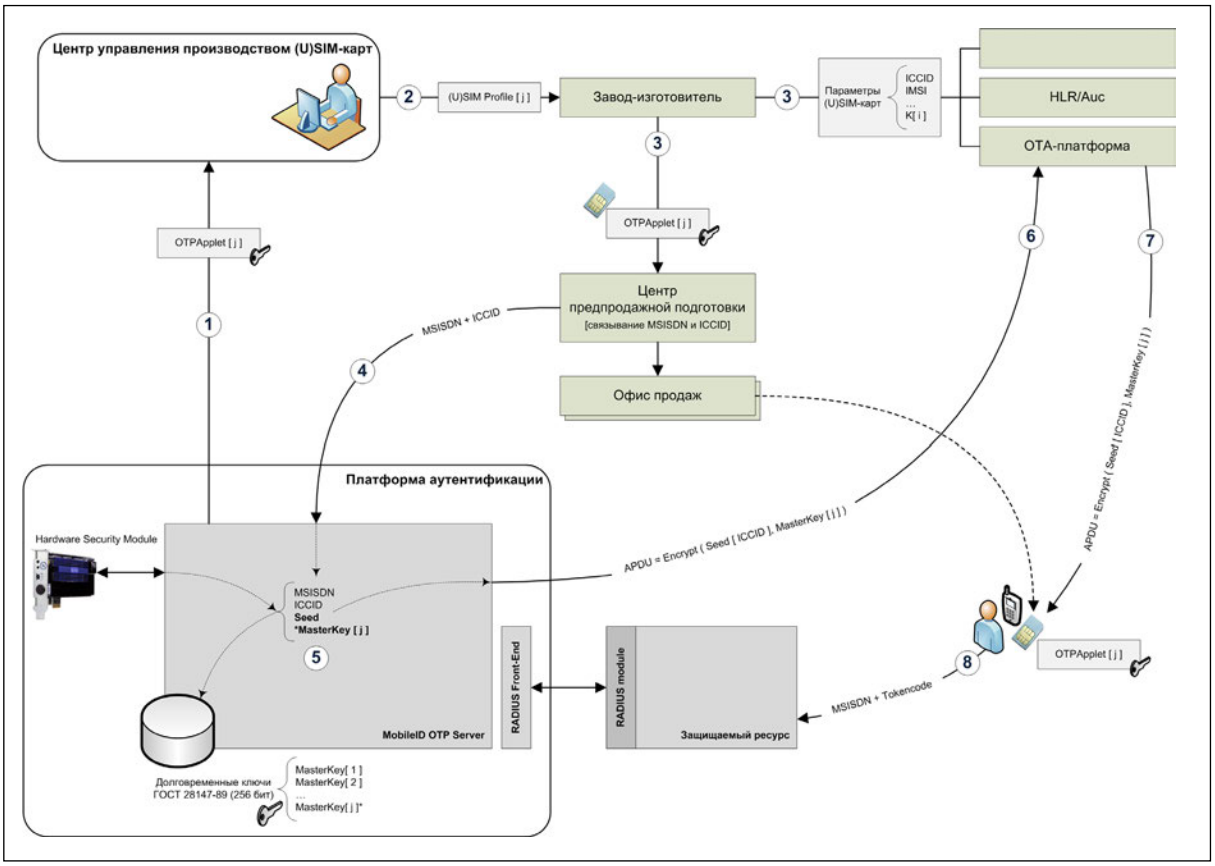

Рис. 3. Схема интеграции системы аутентификации в инфраструктуру оператора связи

В инфраструктуру оператора добавляется платформа аутентификации, средствами которой (с использованием АМБ) генерируется приложение для SIM-карты и необходимый ключевой материал (включая мастер-ключ для защищенного обмена данными с приложением).

Сформированные таким образом апплеты передаются либо в зашифрованном виде, либо по защищенному каналу связи в центр управления производством SIM-карт. В центре управления производством SIM-карт осуществляется формирование профиля SIM-карты для его записи непосредственно на носитель — приложение для генерации одноразовых паролей включается в состав профиля.

Сформированный профиль SIM-карты передается на завод-изготовитель. Выпущенная заводом-изготовителем SIM-карта уже содержит апплет для генерации OTP, однако еще не содержит ключевой материал (начальный вектор генерации), используемый приложением. После того как карта активирована на оборудовании оператора связи, возможна регистрация карты в сети связи и использование установленных на нее приложений.

Выпущенные заводом-изготовителем SIM-карты передаются в центр предпродажной подготовки, где производится формирование абонентских комплектов — брендирование SIM-карт и подготовка информационных материалов, прилагающихся к ним. Здесь же устанавливается соответствие между номером мобильного телефона пользователя MSISDN и номером самой карты ICCID. Таким образом, производится связывание каждой копии приложения для генерации одноразовых паролей с номером мобильного телефона. Номер мобильного телефона на данный момент еще не связан с конкретным физическим или юридическим лицом. Информация о связи номера мобильного телефона и номера SIM-карты передается в платформу аутентификации.

Карта поступает в центр продаж и обслуживания абонентов, где при заключении с абонентом договора о предоставлении услуг связи оператор берет в обработку персональные данные абонента.

После того как абонент активирует полученную SIM-карту, платформа аутентификации генерирует начальный вектор генерации для OTP-апплета. При этом значение вектора зашифровывается с использованием мастер-ключа, соответствующего этой копии приложения, и передается на OTA-платформу для загрузки на SIM-карту. Полученный начальный вектор расшифровывается в защищенной области памяти SIM-карты и сохраняется внутри апплета. Таким образом происходит активация приложения для генерации одноразовых паролей. После активации приложения пользователь может использовать генератор одноразовых паролей в схеме строгой двухфакторной аутентификации для безопасного доступа к защищаемому ресурсу.

Описанная схема сочетает в себе несколько подходов, которые позволяют обеспечить безопасность ключевого материала SIM-карт и приложений на них. В приведенной процедуре обмен чувствительными данными производится только в зашифрованном виде, тем самым исключается их открытое использование вне доверенных модулей.

Таким образом, предложенная система аутентификации, использующая в качестве генератора одноразовых паролей SIM-карту абонента, позволяет достаточно эффективно удовлетворить сформулированные требования и может быть интегрирована в инфраструктуру произвольного оператора мобильной связи.

СПИСОК ЛИТЕРАТУРЫ:

1. RSA One-Time Password Specifications (OTPS). URL: http://www.rsa.com/rsalabs/node.asp?id=2816.
2. HOTP: An HMAC-Based One-Time Password Algorithm (RFC4226). URL: http://tools.ietf.org/html/rfc4226.
3. 3GPP TS 11.11 Specification of the Subscriber Identity Module — Mobile Equipment (SIM-ME) Interface. URL: http://www.3gpp.org/ftp/specs/html-info/1111.htm.