П. О. Джунковский, М. В. Дубовицкая

ОБЕСПЕЧЕНИЕ ЗАЩИЩЕННОГО ДОСТУПА К ИНФОРМАЦИИ МОБИЛЬНЫХ И WEB-КЛИЕНТОВ РАСПРЕДЕЛЕННОЙ БИЗНЕС-СИСТЕМЫ

В настоящее время многие банки, коммерческие организации, платежные системы и дилинговые центры предоставляют своим клиентам разнообразные мобильные сервисы для проведения безналичных расчетов, управления торговыми и банковскими счетами. Использование мобильных устройств в подобных сервисах требует обеспечения аутентификации всех сторон информационного обмена, конфиденциальности передаваемой информации пользователя и безопасности хранимых данных.

Платформа J2ME не имеет достаточных средств, способных обеспечить необходимую безопасность передаваемой и хранимой в мобильном устройстве информации. J2ME, следуя концепции Java, предназначена для разработки прикладных программ и имеет очень ограниченные возможности для низкоуровневого взаимодействия с аппаратной платформой. В частности, лишь небольшое количество моделей мобильных устройств позволяет работать с SIM-модулем абонента напрямую, используя JSR – 77 SATSA. Использование SIM-карты в качестве ключевого контейнера решило бы вопрос хранения ключей, однако на практике, ввиду отсутствия поддержки данной технологии производителями, эта идея так и не нашла своего применения. Кроме того, оператор имеет права удаленного доступа к SIM-модулю абонента. Хранение конфиденциальной информации в хранилище файлов в открытом виде (с помощью RMS API или файлового ввода/вывода FCOP/JSR – 72 FileConnection API) невозможно, так как в случае потери или кражи мобильного устройства доступ к информации может быть получен при помощи стандартных средств.

Сетевая безопасность мобильных телефонов представлена реализацией протокола SSL 1.0 для HTTP, однако имеется только односторонняя аутентификация (аутентификация сервера). При этом используется предустановленный производителем набор доверенных сертификатов. Аутентификация клиента проводится иным образом на уровне приложения (с помощью ввода логина и пароля, используя методы HTTP POST/GET).

Другими словами, перед разработчиком встают следующие проблемы:

- нет возможности так или иначе хранить секретную информацию (в том числе ключевую) в памяти телефона в открытом виде. Телефон может быть украден или потерян;
- нет возможности чтения/записи в память SIM-карты непосредственно из приложения;
- встроенные протоколы безопасной связи имеют ограничения с целью увеличения быстродействия;
- реализация прочих протоколов и криптографических алгоритмов часто ограничена из-за вычислительной способности процессора мобильного устройства.

Предлагаемая платформа позиционируется как основа для построения бизнес-систем для мобильных пользователей на базе платформы J2ME, а также расширения функциональности существующих систем для работы с мобильными клиентами. Основой данной платформы является защищенный протокол, обеспечивающий регистрацию пользователя в системе, двустороннюю («строгую») аутентификацию на базе ИОК и конфиденциальность передаваемой информации. Таким образом, данная платформа ориентирована на использование в системах электронной коммерции, платежных системах, системах мобильного банкинга и других системах, где требуется обеспечение аутентичности пользователя и конфиденциальности данных.

Требования, предъявляемые к данной платформе:

— обеспечение различных способов аутентификации клиента и сервера, в том числе двухсторонней «строгой» аутентификации на базе отечественных криптографических алгоритмов и цифровых сертификатов X.509;

— наличие подсистемы многофакторной аутентификации (в том числе с использованием биометрических данных) на базе мобильного устройства;

— обеспечение конфиденциальности передаваемой информации с помощью отечественных алгоритмов шифрования;

— обеспечение удаленной регистрации пользователей и жизненного цикла ключа;

— независимость от оператора сотовой сети;

— функционирование в общедоступных сетях связи.

Функционирование систем на базе данной платформы возможно в мобильных сетях общего пользования (GSM 2G/2.5G) с распространенной технологией пакетной передачи данных (GPRS/EDGE). При этом затраты на развертывание данной системы минимальны, так как не требуется доступ к оборудованию оператора сотовой связи. Система предназначена для функционирования в открытых IP-сетях.

В качестве клиента данной платформы выступает мобильный J2ME-терминал, web-клиент или же их совокупность, при этом мобильный терминал используется как дополнительный фактор аутентификации при работе с web-клиентом. Предоставляется возможность применения различных способов аутентификации, что расширяет спектр предоставляемых сервисов для пользователей бизнес-системы в зависимости от используемого способа:

1. для мобильного и web-клиента: пользователь аутентифицируется с помощью пары логин/пароль, аутентификация сервера не предусмотрена, данные передаются по открытому каналу;

2. для мобильного клиента: двусторонняя «строгая» аутентификация как клиента, так и сервера на основе цифровых сертификатов X.509 и отечественного алгоритма ЭЦП ГОСТ Р 34.10-94 (по аналогии с SSL версии 1.0 RFC 2246 [1]), канал шифруется на установленном сессионном ключе;

3. для web-клиента: двусторонняя аутентификация по аналогии с п. 2 осуществляется при помощи подписанного Java-апплета. Ключевой контейнер располагается в файловой системе отчуждаемого носителя, канал шифруется на установленном сессионном ключе;

4. для web-клиента: пользователь аутентифицируется с помощью пары логин/пароль и одноразового пароля, полученного при помощи мобильного терминала (см. п. 2), канал шифруется на установленном сессионном ключе;

5. для мобильного и web-клиента: использование биометрических данных на основе цифрового почерка пользователя. Применение биометрии для данных целей является темой будущих исследований и не рассматривается в данной работе.

В качестве мобильного терминала используется мобильное устройство J2ME с поддержкой TCP сокет-соединения (большинство мобильных телефонов, имеющих профиль мобильного устройства MIDP1.0/1.1). Для хранения ключевого контейнера используется локальное хранилище RMS или (если поддерживается устройством) JSR-72 FileConnection API. Ключевой контейнер защищен буквенно-цифровым паролем, чувствительным к регистру букв, и может содержать специальные символы. Ввод пароля пользователем необходим каждый раз при обращении к секретному ключу.

Web-клиентом является web-браузер с поддержкой Java (любой современный браузер).

Серверная часть платформы представляет собой комплекс J2EE-компонентов под управлением сервера приложений JBoss (или другого, например WebSphere). Компонентами системы являются (представлено на рис. 1):

— центр сертификации;
— центр регистрации;
— сервер БД;
— web-клиент пользователя;
— консоль администратора;
— XML-RPC-сервер;
— сетевой шлюз;
— компонент бизнес-логики.

Шлюз обеспечивает взаимодействие с мобильными клиентами по защищенному протоколу. Далее информационный поток пользователей инкапсулируется в XML-RPC-запросы поверх HTTPS. Таким образом, обеспечивается интеграция с другими системами на базе J2EE-платформы, так как нет необходимости встраивания собственных сокет-серверов в J2EE-сервер приложений.

Центр регистрации обеспечивает управление учетными данными пользователей (регистрационная информация пользователя, статус сертификата пользователя, история отозванных сертификатов и т. д.) и взаимодействием с сервером БД (поддерживается широкий спектр БД

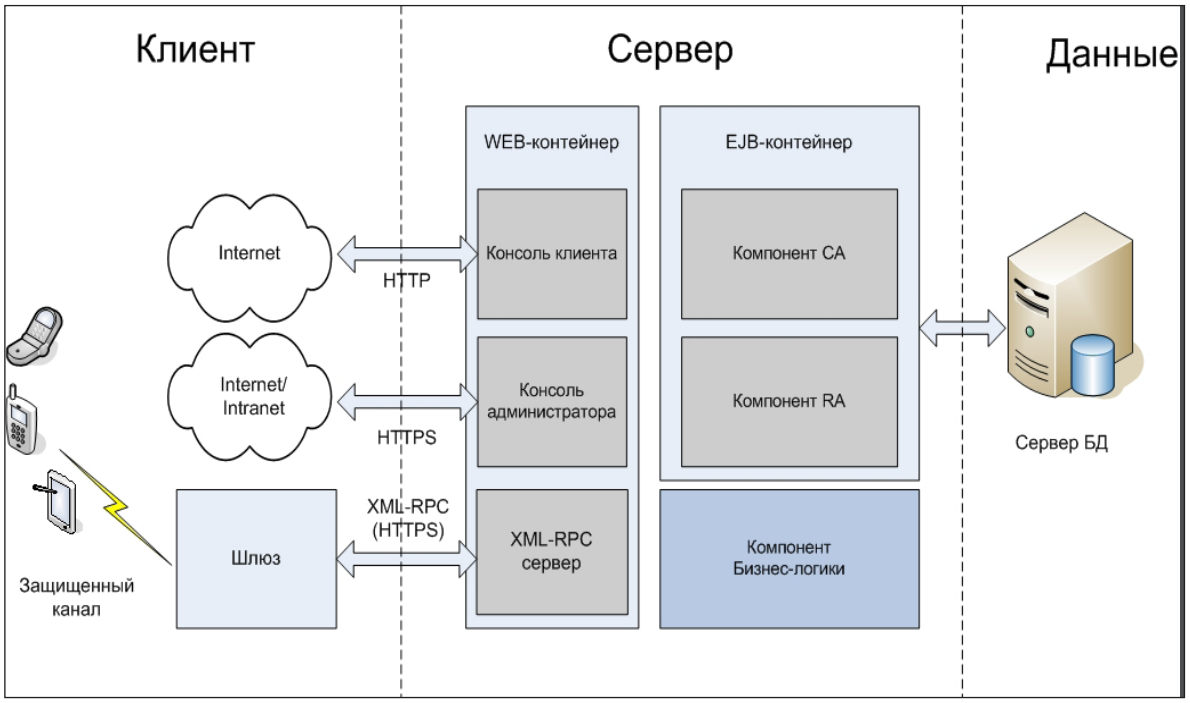

Рис. 1. Архитектура системы

Центр сертификации обеспечивает издание сертификатов пользователей и сертификата аутентификации сервера. В качестве центра сертификации может выступать сторонний сертифицированный ЦС, взаимодействие с которым может быть обеспечено по одному из доступных протоколов.

С помощью web-клиента пользователь системы получает доступ в систему и в зависимости от типа аутентификации получает соответствующие права доступа: информацию о текущем статусе сертификата в случае ввода пользовательского пароля без установки защищенного соединения и полный доступ к системе в случае использования одного из способов «строгой» аутентификации.

С помощью консоли администратора производится управление учетными записями пользователей (добавление новых пользователей, изменение учетных данных пользователей,

установка требуемого типа аутентификации для каждого пользователя и т. п.), изменение статусов сертификатов или их отзыв, а также общее администрирование компонентов системы.

Компонент бизнес-логики представляет собой собственно интерфейс (например, WSDL как стандартный интерфейс взаимодействия сервисов SOA-платформ, RPC или программный интерфейс) взаимодействия с бизнес-системой, для которой обеспечивается безопасность работы с мобильными пользователями.

Регистрация пользователя происходит в два этапа. На первом этапе пользователь получает одноразовый пароль в конверте, с помощью которого будет происходить первичная аутентификация пользователя на сервере. На втором этапе происходит генерация ключевой пары пользователем и создание запроса на сертификат.

После получения запроса сервер получает регистрационные данные пользователя из базы данных и происходит издание сертификата пользователя. Клиенту сертификата отправляется блок данных, состоящий из корневого сертификата Центра Сертификации, сертификата аутентификации сервера и сертификата аутентификации клиента. Данный блок зашифрован с помощью ключа, созданного на базе одноразового пароля. Таким образом, происходит первичная аутентификация сервера на стороне клиента. После получения данного блока данных и сохранения сертификатов в безопасном хранилище одноразовый пароль уничтожается.

После прохождения процедуры регистрации пользователь готов для работы в системе. Перед соединением с сервером пользователь вводит пароль доступа к секретному ключу. Далее клиентское приложение формирует блок аутентификации пользователя, состоящий из собственного сертификата аутентификации и сообщения Diffie – Hellman. Данный блок подписывается на секретном ключе клиента по алгоритму ЭЦП ГОСТ Р 34.10-94 и отравляется серверу. После завершения процесса аутентификации сервер и клиент согласовывают сессионный ключ в соответствии с RFC 4357 [2]. Шифрование передаваемой информации осуществляется с помощью ГОСТ 28147-89 в режиме OFB. В случае разрыва соединения процесс аутентификации пользователя повторяется.

Выбор соответствующих криптографических алгоритмов и алгоритмов ЭЦП связан с оценкой скорости выполнения криптографических операций на мобильных устройствах на базе платформы J2ME. Так, процесс генерации ключевой пары ГОСТ Р 34.10-94 занимает в среднем 30–45 секунд, а процесс подписания и проверки подписи – в среднем 3–5 секунд. Те же показатели для ГОСТ Р 34.10-2001 составляют 20–30 минут и 7–8 минут соответственно, что неприемлемо для использования в мобильных сервисах, которые призваны обеспечивать быстрый повсеместный доступ к сервису.

К особенностям разработанной системы относятся:

1. Поддержка всех мобильных устройств, имеющих профиль MIDP1.0/2.0 с возможностью создания TCP-соединения.

2. Функционирование в стандартных сетях связи.

3. Независимость от оператора сотовой связи.

4. Интегрируемость в существующие J2EE-бизнес-системы.

5. Гибкость развертывания системы в зависимости от требований безопасности бизнес-системы.

6. Поддержка различных способов аутентификации и разграничение на их основе предоставляемых бизнес-системой сервисов.

7. Поддержка методов многофакторной аутентификации, в том числе с использованием биометрических данных пользователя.

8. Модульная архитектура, возможность наращивания функционала системы.

Таким образом, данная платформа может быть интегрирована в существующие корпоративные информационные системы (КИС) на базе SOA-решений Java для организации защищенного

информационного обмена с мобильными пользователями, обеспечивать гибкость предоставляемых сервисов и ресурсов в зависимости от прав доступа и типа аутентификации пользователя, а также быть основой для построения новых КИС.

СПИСОК ЛИТЕРАТУРЫ:

1. *Dierks T., Allen C.* The TLS Protocol Version 1.0. — IETF, RFC 2246, January 1999. URL: http://www.ietf.org/rfc/rfc2246.txt.
2. *Popov V., Kurepkin I., Leontiev S.* Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11 -94 Algorithms. — IETF, RFC 4357. January 2006. URL: http://www.ietf.org/rfc/rfc4357.txt.