УДК 004

Казанский государственный энергетический университет
Студент Э.Р. Галиуллина
Студент А.А. Шакиров
Канд. техн. наук, доцент Р.С. Зарипова,
Россия, г. Казань
E-mail: zarim@rambler.ru

Kazan State Power Engineering University
Student E.R. Galiullina
Student A.A. Shakirov
Cand. tech. Sci., Assoc. R.S. Zaripova,
Russia, Kazan
E-mail: zarim@rambler.ru

Э.Р. Галиуллина, А.А. Шакиров, Р.С. Зарипова

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ФИНАНСОВЫХ ТРАНЗАКЦИЯХ ЧЕРЕЗ МОБИЛЬНЫЙ ТЕЛЕФОН: АЛГОРИТМЫ

**Аннотация:** Сегодня мобильная коммерция рассматривается многими компаниями, бизнесом и организациями. В мобильной коммерции информационная безопасность финансовых транзакций очень важна. Это происходит из-за обмена информацией об учетной записи, включая номер счета, пароль, кредитные счета и т. д. а раскрытие этой информации повлечет за собой большие финансовые и моральные потери. По этой причине следует использовать алгоритмы для их совершения и увеличения защищенности транзакций. Среди этих алгоритмов приложения WAP, J2ME, Toolkit SIM идентифицированы и описаны в этой статье на основе систематического обзора. Кроме того, есть несколько рекомендаций относительно соответствия различным ситуациям для реализации конкретного алгоритма для этой проблемы. Более подробные результаты впоследствии объясняются в этой статье.

**Ключевые слова:** мобильная коммерция, информационная безопасность, финансовый обмен, транзакция, электронная коммерция.

E.R. Galiullina, A.A. Shakirov, R.S. Zaripova

# INFORMATION SECURITY IN FINANCIAL TRANSACTIONS VIA MOBILE PHONE: ALGORITHMS

**Abstract:** Today, mobile commerce is considered by many companies, businesses and organizations. In mobile commerce, information security of financial transactions is very important. This is due to the exchange of information about the account, including account number, password, credit accounts, etc. and the disclosure of this information will entail great financial and moral losses. For this reason, algorithms should be used to complete them and increase transaction security. Among these algorithms, WAP, J2ME, Toolkit SIM applications are identified and described in this article based on a systematic review. In addition, there are several recommendations for matching various situations to implement a specific algorithm for this problem. More detailed results are subsequently explained in this article.

**Keywords:** mobile commerce, information security, financial exchange, transaction, electronic commerce.

В современном мире мобильная коммерция обсуждается как один из наиболее важных вопросов в деловых организациях и компаниях. Мобильная коммерция – это любая транзакция, в которой финансовый обмен осуществляется через сети мобильной связи. Согласно этому определению, мобильная коммерция представляет собой подмножество всей электронной коммерции, включая как бизнес для потребителя, так и бизнес для бизнеса. Мобильная коммерция использует Интернет для покупки товаров и услуг, а также для отправки и получения сообщений с помощью портативных беспроводных устройств. Мобильная коммерция может быть определена, например: любая электронная транзакция или информационное взаимодействие, проводимое с использованием мобильного устройства и мобильных сетей, которое приводит к передаче реальной или предполагаемой ценности в обмен на информацию, услуги или товары [1-3]. Мобильная коммерция предлагает потребителям удобство и гибкость мобильных услуг в любое время и в любом месте. Мобильная коммерция известна как мобильная электронная коммерция или беспроводная электронная коммерция.

Беспроводная связь является более сложной и опасной, чем проводная связь по многим причинам, включая маршруты передачи сигналов и взаимодействие с окружающей средой, звуками и возможным незаконным прослушиванием телефонных разговоров из-за использования радиоволн. Эти проблемы приводят к меньшей пропускной способности, более высокой частоте появления ошибок и повторной неисправности, поэтому качество беспроводной линии связи ниже, чем для проводного соединения. Следовательно, многие компании и организации не желают применять мобильную коммерцию.

Инфраструктуры открытых ключей основаны на криптографии с открытыми ключами, в которой используются два ключа: закрытый ключ, который хранится в секрете, и открытый ключ, который можно разглашать публично. Интересным свойством этой пары ключей является то, что для расшифровки сообщений, зашифрованных одним, нужен другой. Самый популярный алгоритм криптографии с открытым ключом является RSA. Алгоритм эллиптической криптографии начинает получать признание в мобильных устройствах. Они полагаются на различные математические свойства, которые позволяют использовать более короткие ключи, которые обеспечивают более быстрые вычисления, более низкое энергопотребление, меньшие требования к памяти и пропускной способности и, следовательно, довольно привлекательны для мобильных устройств.

Цифровые подписи могут гарантировать подлинность сторон транзакции, целостность и неоспоримость передач. Цифровая подпись создается, когда передаваемый документ шифруется с использованием закрытого ключа. Процесс шифрования документа с использованием закрытого ключа аутентифицирует документ, поскольку документ мог быть зашифрован только с использованием закрытого ключа владельца. Получатели могут проверить подпись, расшифровав с помощью открытого ключа. В реальном мире документы не полностью зашифрованы, чтобы сэкономить время. В таких случаях используются односторонние хэш-функции. Хэш использует одностороннюю математическую функцию для преобразования данных в дайджест фиксированной длины, называемый хэшем, который впоследствии шифруется. Проверка подписи включает воспроизведение хэша, сгенерированного из полученного сообщения, и сравнение его с расшифрованным оригинальным хэшем.

Цифровые подписи не являются достаточными средствами для автоматической проверки, поскольку даже если подпись может быть проверена. Нет гарантии того, что лицо, сделавшее подпись, является тем, кем он себя считает. Сертификаты открытого ключа являются мощным средством установления доверия к криптографии с открытым ключом. Сертификат – это чей-то открытый ключ, подписанный и упакованный для использования в инфраструктуре открытого ключа. Как правило, сертификат содержит следующие три элемента информации: имя субъекта, для которого выдан сертификат; открытый ключ,

связанный с этим субъектом, и цифровая подпись, подписанная эмитентом сертификата. Цифровая подпись будет проверять информацию о сертификате и, если проверка прошла успешно, то гарантируется, что открытый ключ в сертификате действительно принадлежит объекту, к которому относится сертификат.

Рассматриваемые функциональные области, связанные с безопасностью в WAP, включают в себя безопасность беспроводного транспортного уровня (WTLS), модуль беспроводной идентификации, инфраструктуру открытого ключа WAP, текстовую подпись сценария WML и сквозную безопасность транспортного уровня. Протокол WTLS (Wireless Transport Layer Security) – это протокол безопасности с поддержкой PKI, разработанный для защиты связи и транзакций по беспроводным сетям. Протокол WTLS, такой как SSL, является одним из способов защиты WAP-соединения. Он используется с транспортными протоколами WAP для обеспечения безопасности на транспортном уровне между клиентом WAP в мобильном устройстве и WAP-сервером в WAP-шлюзе.

По большей части разработчики WAP используют стандартные протоколы, и широко на всех уровнях в WAP 2.0, из-за нестандартного стека протоколов WAP 1.0. Поскольку WAP основан на IP, на сетевом уровне поддерживается полностью IPsec, а транспортный уровень защищает TCP-соединение с использованием TLS. На верхнем уровне поддерживается HTTP-метод аутентификации. На прикладном уровне имеется система библиотек для шифрования, где размещены средства для точного контроля и неоспоримого сообщения разработчикам WAP. Поскольку WAP 2.0 основан на общепризнанных стандартах, то существует большая вероятность того, что его службы безопасности будут лучше и безопаснее, чем 802.11 и Bluetooth, особенно для служб аутентификации, целостности и конфиденциальности сообщений.

Модуль идентификации абонента GSM (глобальная система мобильной связи), который хранит личные данные абонента, может быть реализован в виде смарт-карты, называемой SIM-картой. SIM-инструментарий – это спецификация SIM-карты и функциональных возможностей терминала, которые позволяют SIM-карте управлять мобильным терминалом для определенных функций. Инструментарий приложения SIM (SAT) используется для создания приложений мобильных платежей на основе службы коротких сообщений (SMS). В системах на основе инструментария SIM-приложения связь между мобильным клиентом и сервером платежей осуществляется с помощью SMS. SMS используется для инициирования и авторизации платежей. Пользователь идентифицируется и аутентифицируется службой аутентификации GSM, и, следовательно, оператор мобильной сети GSM действует как посредник между мобильным клиентом, сервером платежей и продавцом.

Основными преимуществами использования платформы J2ME являются возможность обеспечения динамического контента и информационной безопасности. Кроме того это мощный, объектно-ориентированный язык программирования с большой базой разработчиков. Информационные устройства и другие портативные устройства интегрированы с аудио, мультимедиа, возможностью подключения и услугами, доступными на одной платформе. Растущая и динамичная вычислительная мощность на этих устройствах позволит разработчикам услуг с высокой добавленной стоимостью. Например, местные информационные службы, позволяющие пассажирам подключаться к Интернету с помощью мобильного телефона и получать доступ к необходимой информации, в том числе местонахождению ближайшего отеля, планам и расписанию [4-6]. Одним из приложений мобильной коммерции является использование мобильных платежей на заправке. Успехи этих приложений требуют высокого уровня надежности и безопасности. Мобильные устройства содержат цифровой идентификатор и из-за этого должен быть способ аутентификации пользователей и обеспечения надежности системы. Обеспечение безопасного доступа к данным абсолютно необходимо в мобильной сети. Оно снижает уровень мошенничества в мобильных платежных системах. Современные практики в

платформе J2ME основаны на услугах, предоставляемых в защищенной смарт-карте или аналогичном устройстве, для создания доверия и уверенности в том, что безопасное хранение ключей и криптографических операций и вычислений. Чтобы завершить безопасную транзакцию, продавец должен проверить, авторизованы ли беспроводные подписчики или нет. После этого продавец должен отправить квитанцию подписчику.

По преимуществам и недостаткам введенных алгоритмов и исследований, проведенных в этой области, сделан вывод о том, какие алгоритмы используются в мобильных приложениях, связанных с финансами. Платформа J2ME была бы более подходящей по следующим причинам: выполняется с мобильным обменом, возникают проблемы, включая прослушивание, манипулирование сообщением, генерирование поддельных сообщений и прерывание. Поэтому чтобы избежать этих проблем, необходимы следующие процедуры: аутентификация, конфиденциальность, точность мониторинга и любой способ был бы уместен, который обеспечивает эти четыре решения, а также применим в программах Java из-за достижений в технологии и важности сохранения конфиденциальности информации. В общей сложности платформа J2ME используется для удовлетворения потребностей информационных систем в соответствии с Java software environment. Она предоставляет эти четыре способа. И еще одним преимуществом является то, что эти сервисы могут постоянно обновляться с новыми или улучшенными приложениями, установленными на смарт-карте.

Библиографический список

1. Шакиров А.А. Трансформация систем учета и контроля в условиях цифровой экономики / А.А. Шакиров, Р.С. Зарипова / Наука Красноярья. 2019. – Т. 8. – № 3-2. – С. 112-115.

2. Антипова Т.С. Глобализация и глобальные проблемы в мировой экономике / Т.С. Антипова, А.Р. Залилов, Р.С. Зарипова / «Экономика сегодня: современное состояние и перспективы развития (Вектор-2018)»: Сборник материалов Всероссийской научной конференции молодых исследователей. – Мин-во образования и науки РФ; Росс. гос. ун-т им. А.Н. Косыгина. – 2018. – С. 324-325.

3. Шакиров А.А. Современные информационные технологии как инструмент автоматизации бухгалтерского учета / А.А. Шакиров, Р.С. Зарипова / Наука Красноярья. – 2019. – Т. 8. – № 1-3. – С. 75-78.

Зарипова Р.С. Управление деятельностью организаций в условиях цифровой экономики / Р.С. Зарипова, О.А. Пырнова / Ученые записки ИСГЗ. – 2018. – Т. 16. – № 2. – С. 70-75.

4. Шакиров А.А. Роль новых технологий в экономике XXI века: угрозы и вызовы цифровой экономики / А.А. Шакиров, Р.С. Зарипова / «Экономика сегодня: современное состояние и перспективы развития (Вектор-2018)»: Сборник материалов Всероссийской научной конференции молодых исследователей. – Мин-во образования и науки РФ; Росс. гос. ун-т им. А.Н. Косыгина. – 2018. – С. 331-334.

5. Злыгостев Д.Д. Информационная безопасность как инструмент обеспечения экономической безопасности предприятий / Д.Д. Злыгостев, Р.С. Зарипова / Инновации в информационных технологиях, машиностроении и автотранспорте: Сборник материалов Международной научно-практической конференции. – Кемерово, 2017. – С. 23-25.

6. Шакиров А.А. Актуальность обеспечения информационной безопасности в условиях цифровой экономики / А.А. Шакиров, Р.С. Зарипова / Инновационное развитие экономики. Будущее России: Сборник материалов и докладов V Всероссийской (национальной) научно-практической конференции. – 2018. – С. 257-260.