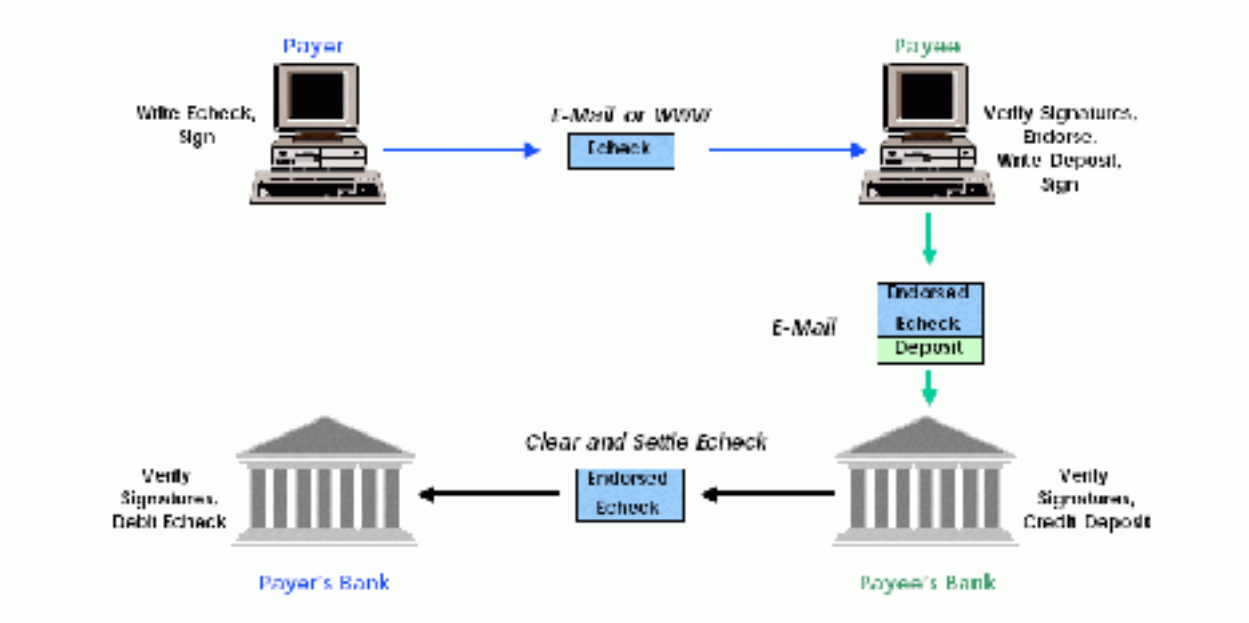
Электронный чек

Вступление

Электронный чек был разработан для выполнения оплаты и других финансовых функций бумажных чеков с помощью использования электронно-цифровых подписей (далее: е-подписи) и безопасной пересылки по сети Интернет. Идея е-чека основана на том, что электронные документы могут заменить бумажные, а е-подписи, зашифрованные методом открытого ключа – рукописные подписи. Для замены бумажного чека е-чеком не требуется создавать новые средства оплаты, как не нужно и вносить и серьезные практические изменения. Е-чек спроектирован таким образом, чтобы как можно лучше влиться в существующую практику чековой оплаты с минимальным негативным воздействием на банки, плательщиков, получателей и на финансовую систему в целом.

Система е-чеков является единственной системой электронных платежей, признаваемой Министерством Финансов США. С ее помощью проводится большинство электронных финансовых операций в США. Ссылка на список компаний, участвовавших в создании этой системы, приведена ниже.

Рис. 1



Основной режим работы

На рис. 1 показан нормальный «рабочий маршрут» е-чека. Плательщик составляет чек посредством составления электронного документа с информацией, которая должна быть в чеке, и зашифровывает ее. Получатель получает е-чек, удостоверяется в подлинности подписи, подтверждает е-чек, выписывает депозит и подписывает его. Банк получателя удостоверяется в подлинности подписей плательщика и получателя, кредитует счет получателя и направляет чек на клиринг и оплату. Банк плательщика проверяет подпись плательщика и дебетует счет плательщика.

FSML

Е-чек включает в себя особую обязательную и иногда произвольную информацию, а также е-подписи. Составляется он на FSML(Financial Services Markup Language) - языке, определенном с помощью SGML(Standard Generalized Markup Language). Структура документа и блоков данных определяется «тэгами», наподобие используемых в HTML, также определяемом языком SGML.

Каждый FSML-документ представляет собой последовательность блоков.

Краткое описание блоков:

<account> Этот блок включает в себя информацию о банковском счете плательщика или получателя. Заполняется представителями банка, в котором открыт счет.
<action> Здесь описываются действия, которые должен выполнить адресат.
<attachment>В этом блоке располагается информация, передаваемая плательщиком получателю.
<bankstamp> Здесь показывается состояние обработки.
<bundle> Здесь располагаются итоги нескольких е-чеков, пересылаемых между банками.
<cashletter> Здесь располагаются итоги кассовых писем, пересылаемых между банками.
<cert> Этот блок включает в себя информацию о сертификате X.509(используется для обеспечения проверяющих подписи открытым ключом шифрования).
<certification> Здесь хранится информация для создания сертифицированного е-чека, наряду с банковскими подписями.
<check> Здесь хранится информация о е-чеке(сумма, дата, когда он подлежит оплате и др.).
<deposit> Здесь располагается информация о е-чеках, которые депонируются целой серией.
<endorsement> Здесь располагается информация, добавляемая индоссантом.
<invoice> Здесь располагается документация по счетам/переводам, информация о платежах, передаваемая от плательщика к получателю.
<signature> Здесь хранится список названий подписанных блоков, список их хэшей, ссылка на сертификат открытого ключа, необходимая для проверки подписи, а также е-подпись, заверяющая весь е-чек.

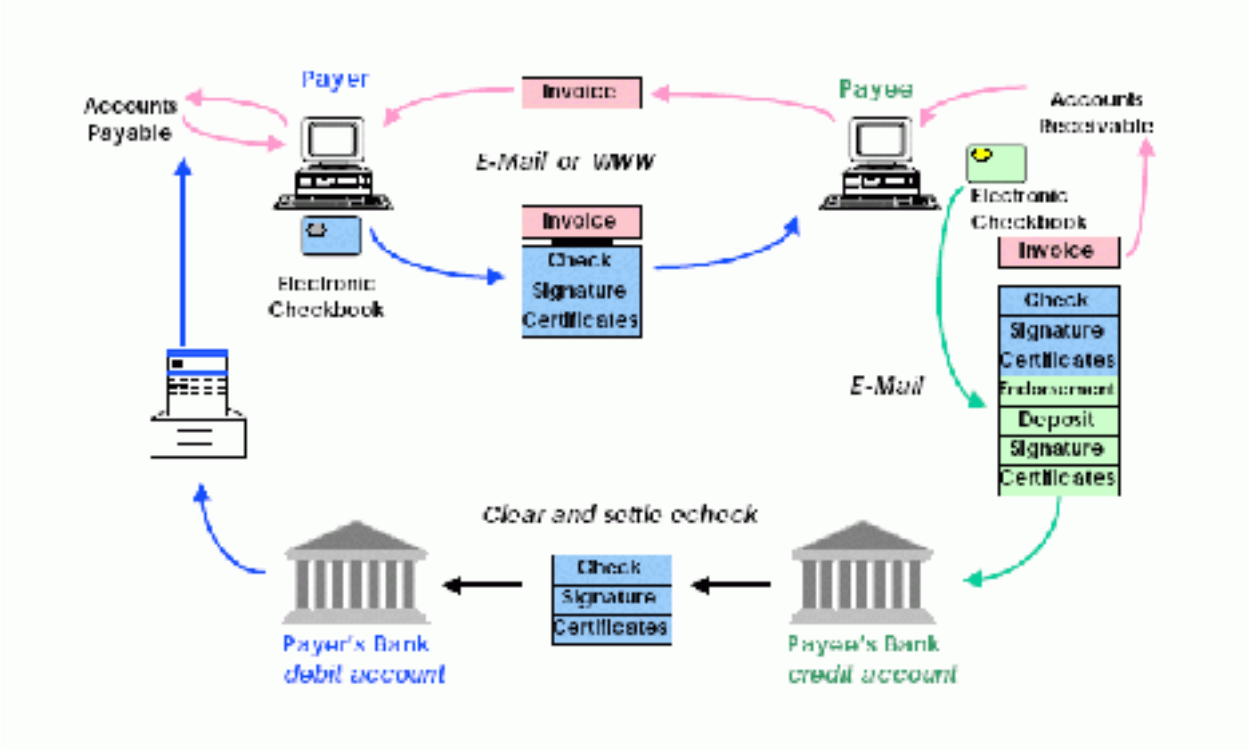
В момент создания е-чек включает в себя минимум информации. Блочная структура, по мере обработки и передачи е-чека от одного лица к другому, позволяет добавлять(или откреплять) все больше и больше информации и подписей. Так, е-чек может быть: создан плательщиком, подписан со-плательщиком, сертифицирован банком, подтвержден получателем, подтвержден со-получателем, депонирован и оплачен. Часть дополнительной информации, например, о сертификации или подтверждении, сохраняется в неприкосновенности, пока е-чек не вернется к плательщику. А, например, бланк денежного перевода может быть прикреплен к е-чеку временно, затем откреплен и обработан отдельно.

Смарт-карта

Для защиты секретного ключа подписи от краж и неправильного использования применяется смарт-карта. Использование криптографического ПО дает проверяющему подлинность подписи больше уверенности, что е-чек пришел от законного хозяина счета, так как секретный ключ генерируется с помощью крипто-алгоритмов, соответствующих банковским стандартам, и используется только в смарт-карте. Секретный ключ шифрования никогда не передается на компьютер клиента и никогда не подвергается угрозе кражи по сети. Электронная чековая книжка также автоматически нумерует каждый чек, когда он выписывается(для того, чтобы отслеживать уникальность е-чеков) и сохраняет лог выписанных чеков, чтобы была возможность свериться, когда возникают вопросы, был ли данный е-чек выписан, подтвержден или депонирован. Использование е-книжки контролируется с помощью ввода PIN'а владельца(более подробно о функциях смарт-карты как чековой книжки будет рассказано ниже).

Е-подписей достаточно для обеспечения безопасности благодаря проверке целостности сообщения, удостоверению подлинности и оригинальности происхождения. Таким образом, система е-чеков и криптография на прикладном уровне может быть экспортирована и использована на международном уровне. Если требуется конфиденциальность между двумя сторонами, шифрование может быть использовано на транспортной линии.

Рис. 2

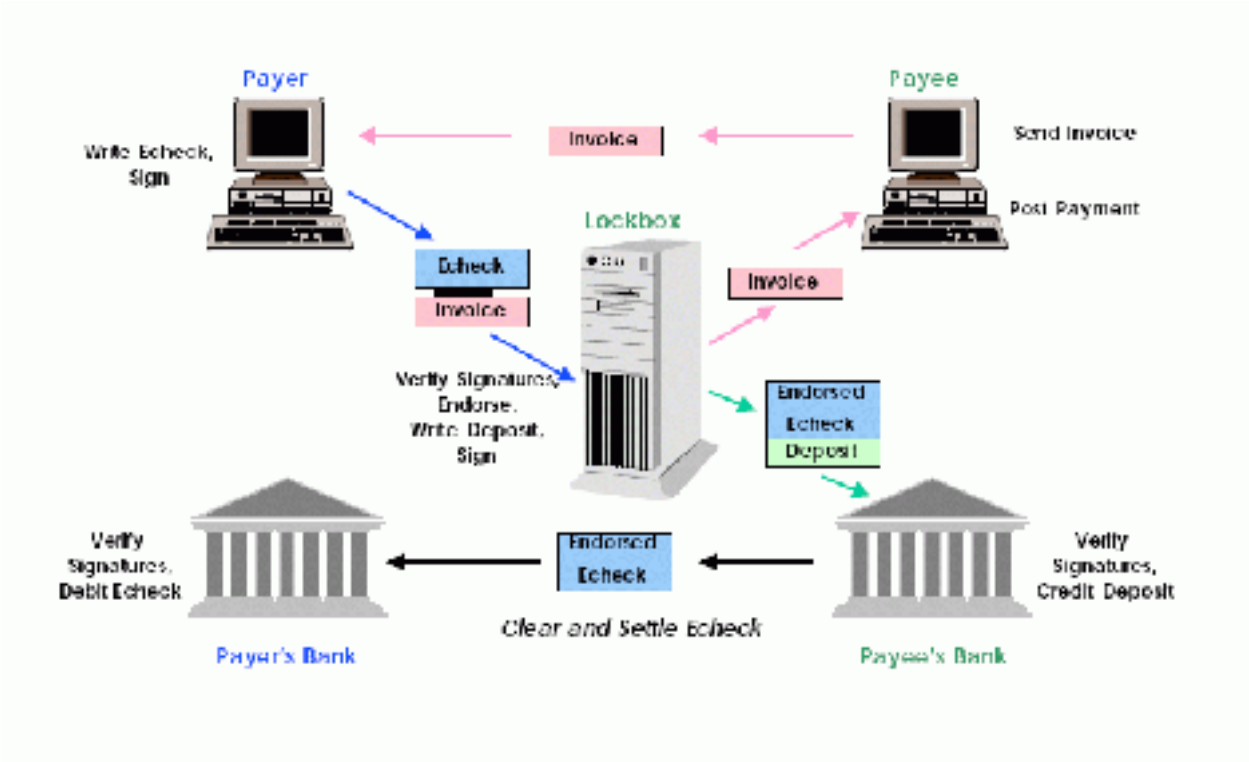


В примере с Рис. 2 транзакция начинается с того, что получатель посылает плательщику счет, который обрабатывается системой оплаты счетов плательщика. Когда приходит время оплатить счет, информация о нем извлекается из системы, и данные счета используются для создания е-чека. В е-чек включается такая информация, как имя получателя, сумма, дата и информация о банковском счете. Для оплаты чека используется смарт-карта. Эта карта хранит в себе секретный ключ шифрования плательщика и гарантирует высокий уровень безопасности. С помощью подписи к е-чеку может также прикрепляться копия счета, так что злоумышленник не сможет подменить счет. Эти мероприятия обеспечивают получателя всей информацией, необходимой для правильной оплаты чека.

Подписанный е-чек и счет посылаются получателю е-мэйлом или веб-транзакцией. Получатель удостоверяет подлинность подписи плательщика на е-чеке и счете, открепляет информацию о счете и запрашивает оплату на счета к получению. Получатель вводит свой PIN и использует свою е-книжку, подтверждая е-чек и подписывая электронный бланк для депонирования серии е-чеков.

Подтвержденный е-чек перенаправляется в банк получателя для депонирования и последующего клиринга. Процедура клиринга может быть выполнена посредством интеграции е-чека в существующие системы Представления Электронных Чеков или других систем клиринга и расчета. И банк получателя, и банк плательщика проверяют все подписи на е-чеке и подтверждении, используя 2-уровневую систему сертификатов, которая «связывает» ключи проверки подписей с подписавшимся и его банковским счетом. Оплачивающий банк убеждается, что эта пересылка е-чека не является дубликатом, что сертификат плательщика и его счет рабочие, и отправляет е-чек на DDA (Demand Deposit Account) плательщика.

Рис. 3



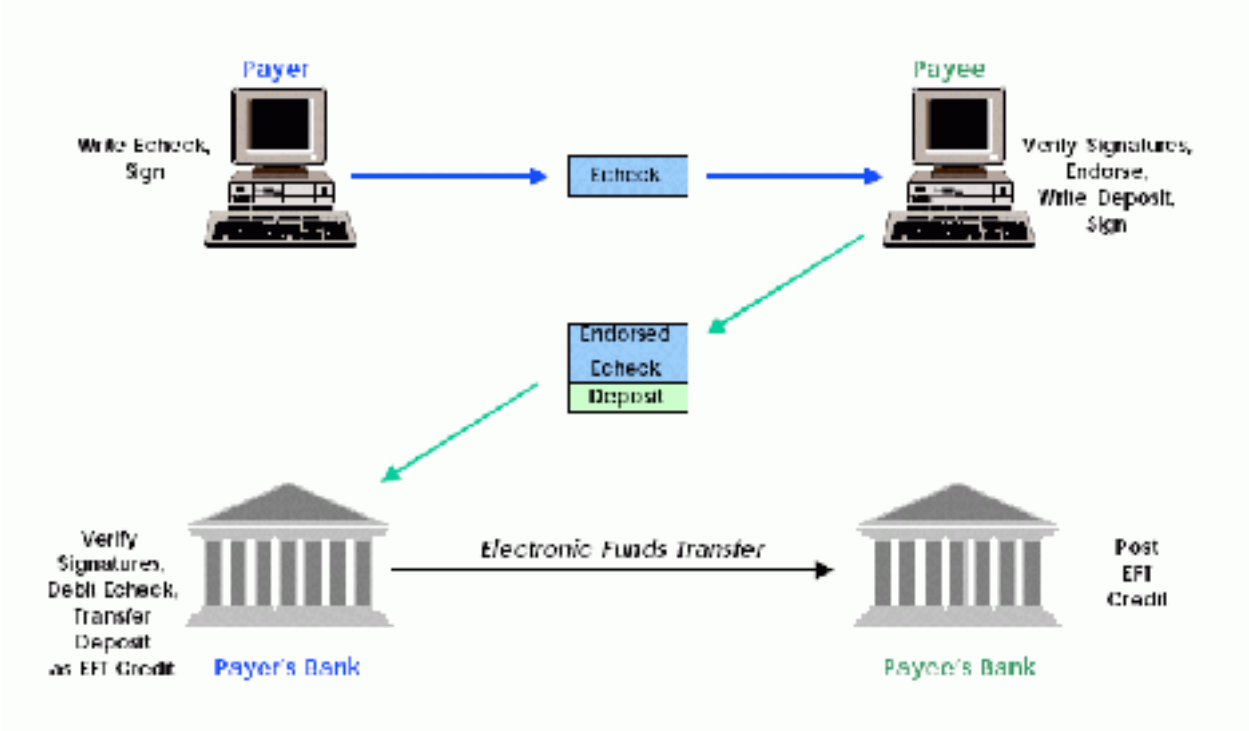
Альтернативные режимы работы

Тип работы системы, показанный на Рис. 2, является самым распространенным способом, но е-чеки можно использовать и иначе, так же как и бумажные чеки.

На рис. 3 показано, как оператор локбокса(сервера, выступающего посредником между плательщиком и пользователем) может обрабатывать е-чек на полпути к получателю. В этом случае, оператор производит крипто-обработку для проверки подписи плательщика на подлинность. Счет или извещение с информацией об оплате могут быть переделаны оператором в тот же формат, что используется для бумажных чеков. Это позволяет получателю получить деньги по е-чеку без применения ПО и аппаратных средств, необходимых для фукнционирования системы е-чеков. Оператор локбокса подтверждает и депонирует е-чек на полпути к получателю. Если локбокс управляется банком получателя, то функции локбокса могут быть переданы банковскому е-чек-серверу, избегая очередного подтверждения и подписывания депозита.

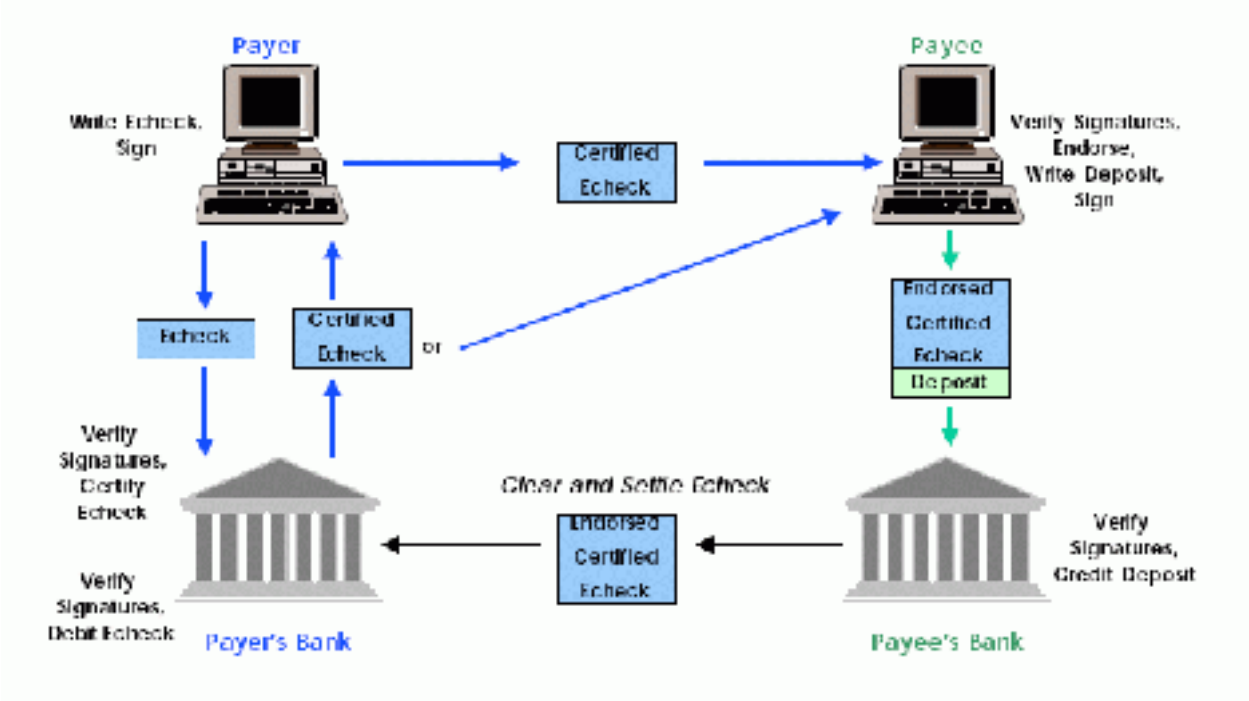
На рис. 4 показано, как получатель может подтвердить и обналичить е-чек в банке плательщика. Банк плательщика отправляет деньги в банк получателя посредством системы электронных платежей. Этот способ особенно полезен, если плательщик желает заплатить получателям, чьи банки еще не поддерживают систему е-чеков. Банк плательщика может предоставить получателю е-книжку, с помощью которой можно обналичивать чеки плательщика.

Рис. 4



На рис. 5 показан метод работы с сертифицированным е-чеком. В этом случае, плательщик посылает е-чек в свой банк. Банк удостоверяется в подлинности подписи плательщика, определяет, достаточно ли средств на его счете, и замораживает счет. Затем банк скрепляет чек подписью для сертификации, и отправляет чек обратно плательщику. Иначе, банк может послать сертифицированный чек напрямую получателю, возможно, через защищенный канал для обеспечения высокой степени защиты и конфиденциальности.

Рис. 5



Электронные чековые книжки

Рукописная подпись является результатом рефлективного движения мышц подписывающегося и в некоторой степени его биометрической характеристикой. Поэтому подделать такую подпись сложно, даже если злоумышленник имеет образец подписи.

Однако, превосходную подделку е-подписи может выполнить кто угодно, для этого достаточно знать секретный ключ шифрования клиента.

Поэтому, важно основывать систему е-чеков на подписях с открытым ключом, когда получатели и банки вынуждены верить, что плательщики могут контролировать использование своих секретных ключей шифрования постоянно. Смарт-карты используются для проверки того, что подписи делаются только законными владельцами, затрудняя тем самым подделку чеков. Карты также стандартизируют и упрощают генерацию ключа, распространение и использование, так что высокий уровень надежности может быть достигнут вне зависимости от опыта и старательности пользователей.

Проверяющий подписи должен быть уверен, что только подписавшийся знает ключ. Если злоумышленник сможет узнать ключ, тогда он сможет подделать подписи, используя свой собственный ПК и Интернет. Если злоумышленник сможет получить контроль над компьютером клиента, то появится возможность подделывать чеки вообще без ведома последнего.

Е-книжка выполняет алгоритм подписи так, что секретный ключ всегда хранится на защищенных устройствах и никогда не считывается уязвимым ПК, подключенным к сети. Также она ведет логи для обеспечения пользователя точными данными о всех действиях с подписями.

Проверяющий подписи должен быть уверен, что пара ключей была сгенерирована таким образом, что секретный ключ не может быть получен или угадан на основе знания открытого ключа.

Проверяющий подписи должен быть уверен, что открытый ключ, предназначенный для проверки подписи на подлинность, действительно принадлежит клиенту, и что он действительно является ключом этой пары.

Также в функции е-книжек входит:

включать уникальный номер книжки(указываются производитель, модель и серийный номер) в каждый е-чек;

последовательно нумеровать каждый е-чек после подписывания, для сохранения уникальности;

генерировать случайные числа для префиксов к блокам чека для повышения безопасности хэш-функций;

выборочно прикреплять персональные данные клиента;

отдельно разблокировывать возможность написания е-чека, администрирования книжки и т.д. с помощью PIN’а;

деактивироваться при краже PIN’а.

Кроме того, е-книжка спроектирована таким образом, что секретный ключ не может быть извлечен путем подключения, и любая успешная попытка получить секретный ключ приведет к внешним повреждениям книжки и выведет ее из строя.

Основной целью при разработке системы е-чеков было предотвращение краж и мошенничеств не полагаясь на шифрование, так как возможность широкого использования шифрования ограничивается экспортным контролем и попытками регулировать использование подобных типов шифрования.

Уникальность каждого чека гарантируется, так как на этом основаны принципы работы е-книжки. Получатель и его банк должны отслеживать и отклонять дубликаты, оплачивая только один экземпляр е-чека. Это предотвращает множественные выплаты, которые могли бы произойти из-за случайных повторных отсылок е-мэйла, а также оплату и депонирование е-чека по двум различным банковским счетам.

Блок чека поддерживает возможность выписывания чеков на банковский код маршрута, на банковский счет или на ИН клиента. Также можно выписывать е-чек на открытый ключ получателя. Эти параметры единственным образом определяют получателя, не позволяя тем самым злоумышленнику нарушать однозначность идентификации получателя путем использования того же имени.

Блоки счета и приложения могут быть посланы с блоками е-чека для описания оплаты. Эти блоки могут быть скреплены электронной подписью, которая прикрепляет эти документы к е-чеку и удостоверяет их подлинность и целостность. Это не позволяет, например, злоумышленнику перехватывать е-чек и заказ на поставку, изменяя адрес доставки в заказе и направляя е-чек и измененный заказ торговой фирме.

Литература:

Architectural Overview
http://www.echeck.org/overview/echecktech.html

Список компаний, участвовавших в разработке системы «Е-чек»:
http://www.echeck.org/overview/consortium/index.html