

# ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ И АУТЕНТИФИКАЦИИ ФИНАНСОВЫХ ТРАНЗАКЦИЙ

Сергей Головашич

Харьковский национальный университет радиоэлектроники,  
пр. Ленина 14, Харьков, Украина, [sgolov@gmail.com](mailto:sgolov@gmail.com), <http://www.kture.kharkov.ua>

**Реферат:** В статье представлена сравнительная характеристика современных технологий аутентификации на основе смарт-карт, отмечены недостатки каждой из рассматриваемых технологий и предложена схема динамической аутентификации, позволяющая устранить основные выявленные недостатки. Также приводится обоснование целесообразности применения NFC-технологии для построения систем аутентификации, обеспечивающих максимальную защиту пользователя от злоупотреблений со стороны обслуживающего персонала системы.

**Ключевые слова:** информационная безопасность, криптография, аутентификация, смарт-карта, Near Field Communication (NFC).

## 1. ВВЕДЕНИЕ

В современных условиях интенсивной автоматизации и информатизации различных сфер деятельности общества, необходимым условием построения жизнеспособных финансово-экономических информационных систем является применение адекватных средств информационной безопасности. Одним из основных требований, предъявляемых к финансовым информационным системам является обеспечение контроля целостности информации, обрабатываемой в системе, на всех этапах её жизненного цикла. Информационная система может рассматриваться как безопасная, если используемые в ней средства и технологии защиты информации позволяют предотвратить либо обнаружить попытки несанкционированного доступа (НСД) со стороны *любого* потенциального злоумышленника.

На сегодняшний день, во всём мире широкое распространение получили технологии идентификации и аутентификации субъектов платёжных (информационных) систем на основе пластиковых карт, однако, многие из используемых сегодня технологий уже не отвечают современным требованиям безопасности. При этом последнее утверждение справедливо даже применительно к наиболее прогрессивным *смарт-технологиям* [1].

Целью данной лекции является краткий анализ недостатков (уязвимостей) применяемых сегодня технологий идентификации и аутентификации на базе смарт-карт, определение возможных угроз и предложение по их перекрытию. В дальнейшем изложении мы

сосредоточим наше внимание на платёжных карточных системах, как наиболее привлекательном объекте IT-мошенничества, однако всё ниже сказанное справедливо по отношению к любым сферам применения систем идентификации и аутентификации на базе смарт-карт [2,3]. Вопросы обеспечения конфиденциальности данных хранящихся на картах подробно рассматривать не будем, т.к. эта задача имеет второстепенное (после аутентификации) значение и может быть решена достаточно тривиально.

## 2. ДВА ТИПА ТРАНЗАКЦИЙ

В настоящее время, в платёжные системы на базе пластиковых карт могут поддерживать два основных типа транзакций: *on-line* и *off-line*.

Системы, ориентированные на поддержку только *on-line* транзакций предполагают наличие постоянного канала связи между финансовым терминалом и сервером банка-эмитента. В этом случае процедура авторизации выполняется на сервере банка и разрешение на завершение транзакции выдаётся сервером банка. Такое решение является наиболее безопасным, однако предъявляет жёсткие требования к качеству и надёжности используемых каналов связи. С другой стороны, в таких системах может использоваться достаточно простое терминальное оборудование и карты с магнитной полосой.

Системы, предусматривающие поддержку *off-line* транзакций, не требуют наличие постоянного канала связи между финансовым терминалом и серверами банка-эмитента. В этом случае процедура авторизации выполняется

непосредственно на терминале. Такое решение потенциально является менее безопасным, однако более предпочтительно с точки зрения оперативности обслуживания пользователей и сокращения накладных расходов на выполнение отдельной транзакции. Поэтому поддержка *off-line* транзакций является необходимым условием построения современной системы электронных платежей. Однако для реализации такой системы необходимо применение смарт-карт и более сложного терминального оборудования.

### 3. УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Рассмотрим технологии обеспечения контроля целостности, применяемые в обоих типах систем.

Для упрощения дальнейшего изложения воспользуемся следующими обозначениями:

$X$  – данные хранящиеся на карте (и подлежащие аутентификации);

$P$  – персональный идентификационный номер (ПИН) карты;

$I_i$  – уникальный идентификатор субъекта системы;

$E_i$  – секретный ключ формирования цифровой подписи (ЦП);

$D_i$  – открытый ключ проверки цифровой подписи;

$C_i$  – сертификат открытого ключа  $D_i$  (открытый ключ подписанный доверенной стороной);

$S_i$  – цифровая подпись, сформированная на ключе  $E_i$ ;

Основные преобразования будем обозначать следующим образом:

$H()$  – однонаправленная функция хеширования;

$F_k()$  – симметричное шифрование на ключе  $k$ ;

$S_i()$  – формирование цифровой подписи на секретном ключе  $E_i$ ;

$E_i()$  – формирование цифровой подписи  $S_i$  (либо сертификата  $C_j$  открытого ключа  $D_j$ ) на секретном ключе  $E_i$ ;

$D_i()$  – проверка цифровой подписи  $S_i$  на открытом ключе  $D_i$  (либо проверка целостности сертификата  $C_j$  и извлечение из него ключа  $D_j$ );

(P)RNG – датчик (псевдо-) случайных чисел.

Общая структура сертификата:

$$C_j = E_i(X_j) \quad C_j = \{F_k(X_j) \parallel S_i\} \quad S_i = S_i(X_j)$$

где ключ  $k$  симметричного шифрования  $F_k$  является фиксированным (при статической аутентификации) либо формируется по схеме класса Диффи-Хеллмана (при динамической аутентификации).

Субъектов системы будем обозначать с помощью следующих индексов:

$p$  – процессинговый центр;

$e$  – банк-эмитент карт;

$c$  – пользователь (карта).

## 4. ТИПЫ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ ДАННЫХ НА КАРТЕ

Различают два типа аутентификации: статическую и динамическую.

*Статическая аутентификация* предполагает односторонний контроль целостности – только терминальное оборудование проверяет целостность карточки. В этом случае могут использоваться карты с магнитной полосой.

*Динамическая аутентификация* предполагает двусторонний контроль целостности – не только терминальное оборудование проверяет целостность карточки, но и карточка проверяет подлинность терминала. В этом случае карточки должны строиться на основе микропроцессора оснащённого внутренней памятью и способного выполнять криптографические преобразования. Такие карты получили название смарт-карт.

Рассмотрим оба способа аутентификации.

## 5. СТАТИЧЕСКАЯ АУТЕНТИФИКАЦИЯ

Статическая аутентификация в *on-line* системах (а также внутрибанковских (одно-эмитентных) *off-line* системах) может строиться на основе симметричных криптоалгоритмов. Однако, для построения глобальной (многоэмитентной) системы электронных платежей с поддержкой *off-line* транзакций, требуется применение асимметричных криптоалгоритмов цифровой подписи. В силу универсальности второго варианта статической аутентификации рассмотрим подробнее именно его.

*Асимметричная статическая аутентификация*

Эмитент формирует пару ключей цифровой подписи: секретный ( $E_e$ ) и открытый ( $D_e$ ). Секретный ключ хранится в секрете, а открытый ключ помещается в платежные терминалы.

В процессе персонализации карт на них записываются постоянные данные: номер карты, срок её действия, информация о владельце и возможно другая служебная информация. В двоичном виде, конкатенация этих данных представляет собой некоторый двоичный вектор  $X$ .

Для заданного вектора  $X$  и ПИН-кода  $P$

владельца карты, эмитент, с помощью собственного секретного ключа  $E_e$ , вычисляет цифровую подпись карточки  $S_c = E_e(H(X \| P))$ , которая и является аутентификационным значением данной карты. Это значение также помещается на карту.

При обслуживании карты в платежной точке терминал, получив с карты значения  $X$  и  $S_c$ , выполняет проверку цифровой подписи эмитента  $D_e(S_c, H(X \| P))$ . Только если цифровая подпись верна, карта считается аутентичной и принимается к обслуживанию.

Достоинством такой аутентификации

является ее простота, а недостатком сложность создания много-эмитентных платежных систем, поскольку открытые ключи всех эмитентов должны "знать" **все платежные терминалы**. Даже если это можно обеспечить, то при появлении нового эмитента возникают значительные трудности в рассылке его открытого ключа всем терминалам. Кроме этого ключ эмитента в этой схеме не сертифицирован и это несколько её ослабляет.

Другая схема статической аутентификации (Рис. 1) устраняет последний недостаток, но несколько усложняет протокол.

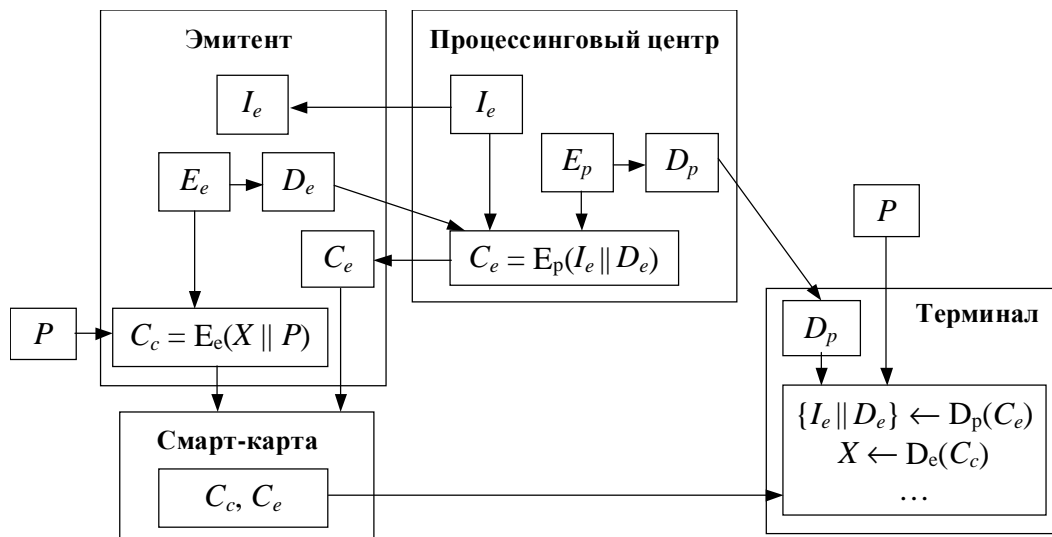


Рис.1. Статическая аутентификация с сертификацией открытого ключа эмитента

Данная схема аутентификации позволяет создавать много-эмитентные платежные системы. Каждый эмитент создает свою пару ключей ( $E_e, D_e$ ). Открытые ключи  $D_e$  передаются в процессинговый центр для сертификации. Процессинговый центр выделяет каждому эмитенту идентификатор  $I_e$ , который конкатенируется с открытым ключом соответствующего эмитента, а затем ключ и идентификатор подписываются секретным ключом процессингового центра  $C_e = E_p(I_e \| D_e)$ .

Полученный сертификат передается эмитенту. При персонализации карт эмитент подписывает данные карты  $X$ , объединённые с ПИН-кодом  $P$ , своим секретным ключом  $E_e$  и полученную цифровую подпись карты  $S_c = E_e(X)$  вместе с сертификатом  $C_e$  своего открытого ключа  $D_e$  помещает на карту.

Процессинговый центр снабжает все терминалы своим открытым ключом.

При обслуживании карты терминал с помощью открытого ключа процессингового центра получает идентификатор эмитента и его открытый ключ  $\{I_e \| D_e\} \leftarrow D_p(C_e)$ . Затем с помощью открытого ключа эмитента  $D_e$  он

проверяет цифровую подпись эмитента  $D_e(S_c) \stackrel{?}{=} 1$ . Если цифровая подпись верна, то терминал принимает карту к обслуживанию, иначе он ее отвергает.

#### Достоинства

В данной схеме каждая из сторон (эмитент, процессинговый центр, терминал) знает только открытые чужие ключи. Секретные ключи известны только их владельцам. Это свойство определяет преимущества данной схемы над системами с симметричной аутентификацией:

1. Возможность построения много-эмитентных систем.
2. Простота добавления новых эмитентов и ввода нового терминального оборудования.

#### Недостатки

1. Возможность создания дубликата карты или несанкционированной «повторной передачи» (повторной транзакции).
2. Отсутствие защиты пользователя от злоупотреблений со стороны персонала, обслуживающего терминальное оборудование.

3. Отсутствие защиты пользователя от злоупотреблений со стороны сотрудников банка.

Надёжность рассмотренной схемы может быть увеличена, если корректное завершение транзакции включает наложение цифровой подписи терминала на информацию о выполненной транзакции (подлежащую отправке в банк-эквайер).

## 6. ДИНАМИЧЕСКАЯ АУТЕНТИФИКАЦИЯ

Динамическая аутентификация увеличивает стойкость протоколов обмена данными между терминалом и картой. Динамическая аутентификация может строиться как на базе симметричных, так и асимметричных криптоалгоритмов. Она предполагает, что карта наделена достаточно высоким «интеллектом». В

частности, карта должна уметь выполнять шифрование с помощью симметричного криптоалгоритма и/или выполнять формирование и проверку цифровой подписи.

Суть динамической аутентификации заключается в том, что не только терминал проверяет целостность платёжной карты, но и карта пользователя в состоянии проверить подлинность терминала.

### Симметричная динамическая аутентификация

На Рис. 2 и Рис. 3, изображены схемы так называемых внешней и внутренней аутентификации. В этих схемах в протоколе аутентификации участвуют две карты: карта пользователя и так называемая мастер-карта. Мастер-карта постоянно находится в терминале и может быть физически недоступна извне.

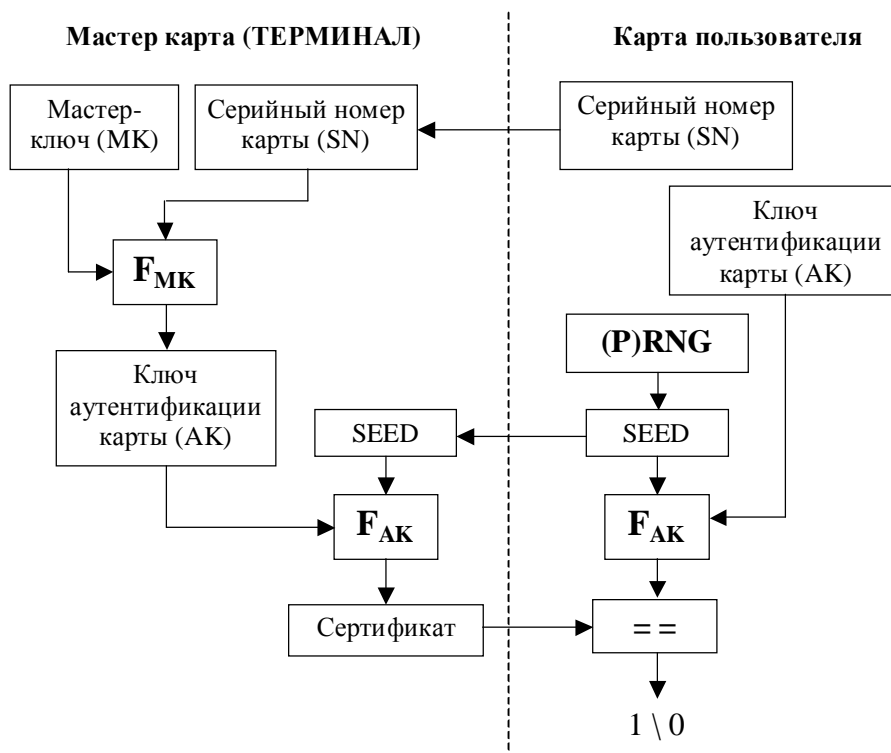


Рис. 2. Внешняя аутентификация. Карточка пользователя проверяет подлинность терминала

В этой карте хранится мастер-ключ, который недоступен из внешнего мира и попадает на нее при персонализации. Обычно для внешней и внутренней аутентификации используются различные мастер-ключи.

В приведенных протоколах динамической аутентификации (Рис. 2 и Рис. 3) в обмене сообщениями между картой пользователя и терминалом присутствует параметр SEED, который представляет собой случайное (или псевдослучайное) число необходимой длины.

Это позволяет сделать неэффективной атаку на протокол, основанную на прослушивании линии с целью повторной передачи ответных пакетов, поскольку в каждом сеансе это значение будет другим. Таким образом, основным требованием к параметру SEED является отсутствие повторений в заданном диапазоне обращений, поэтому для формирования таких значений может использоваться простой датчик ПСП, построенный на базе «счётчика».

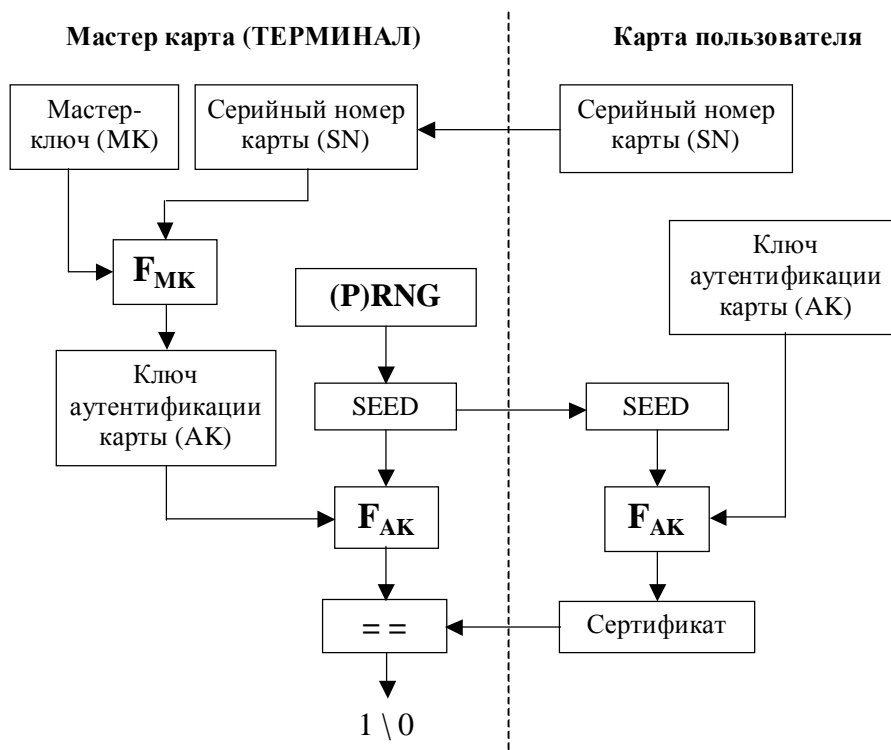


Рис. 3. Внутренняя аутентификация. Терминал проверяет подлинность карты пользователя.

Данные протоколы предполагают, что карта пользователя "умеет" только шифровать в соответствии с некоторым симметричным алгоритмом.

*Достоинства:*

1. Невозможность (высокая технологическая сложность) создания дубликата карты.
2. Защита от злоупотреблений со стороны персонала, обслуживающего терминальное оборудование.
3. Простота и низкая стоимость реализации.

*Недостатки:*

1. Невозможность построения много-эмитентных систем.
2. Отсутствие защиты пользователя от злоупотреблений со стороны сотрудников банка.

**Асимметричная динамическая аутентификация**

Карты, работающие на основе приведенных протоколов (Рис. 2, Рис. 3) можно отнести к картам средней сложности. Карты высшей сложности "умеют" выполнять не только симметричное шифрование но и формировать / проверять цифровую подпись (а также выполнять направленное шифрование либо выработку общего секрета), т.е. поддерживают асимметричную криптографию.

Среди подобных смарт-карт особый интерес

представляют карты, содержащие аппаратные датчики случайных чисел (RNG), т.к. на основе таких карт возможно построение систем с минимальным «уровнем доверия» между субъектами системы. Для этого необходимо чтобы формирование всех секретных ключей в системе выполнялось по принципу «каждый сам себе», т.е. секретный ключ любой карты должен формироваться внутри карты и никогда не выходить за её пределы. Для поддержки данной функциональности карта должна уметь формировать ключевую пару  $\{E_j, D_j\}$  (для схем класса Эль-Гаммала эта задача использует тот же мат. аппарат, что и процедуры формирования / проверки ЦП, поэтому не требует дополнительных аппаратных затрат). Рассмотрим наиболее перспективную схему подсистемы аутентификации на базе смарт-карт последнего типа.

Рекомендуемая схема динамической аутентификации на основе смарт-карт второго типа приведена на Рис. 4.

На приведенном рисунке процедуры инициализации элементов системы и аутентификации отдельной транзакции отделены пунктирной линией. Рассмотрим каждую из процедур подробно.

На этапе инициализации системы процессинговый центр, отвечающий за поддержку работоспособности системы, выполняет начальную прошивку, как пользовательских карт, так и терминальных

мастер-карт, в ходе которой в карточки записываются уникальный идентификатор карты ( $I_c$  или  $I_t$ ) и открытый ключ проверки цифровой подписи процессингового центра  $D_p$ .

При подключении к системе нового банка-эмитента процессинговый центр присваивает ему уникальный идентификатор  $I_e$  и выполняет сертификацию его открытого ключа ЦП  $D_e$ , соответствующий секретный ключ  $E_e$  формируется самим эмитентом и не покидает его пределов.

При добавлении нового пользователя в систему, банк-эмитент выполняет персонализацию карты пользователя, в ходе которой: в память карты записывается необходимая информация о пользователе, на поверхность пластиковой карты наносится

информация о владельце и банке-эмитенте. Затем на специальном стенде пользователь вводит свой ПИН-код  $P$  и инициирует формирование ключевой пары карты  $\{E_c, D_c\}$ , которая формируется с помощью встроенного датчика случайных чисел RNG и сохраняется в защищённой памяти карты вместе с ПИН-кодом  $P$ . После этого открытый ключ карты сертифицируется (подписывается) секретным ключом банка-эмитента  $E_e$  и в виде сертификата  $C_c$ , вместе с сертификатом открытого ключа эмитента  $C_e$  записывается в энергонезависимую память карты. На этом процедура персонализации карты завершается.

Аналогичным образом выполняется формирование, сертификация и загрузка сертификата для терминальной карты.

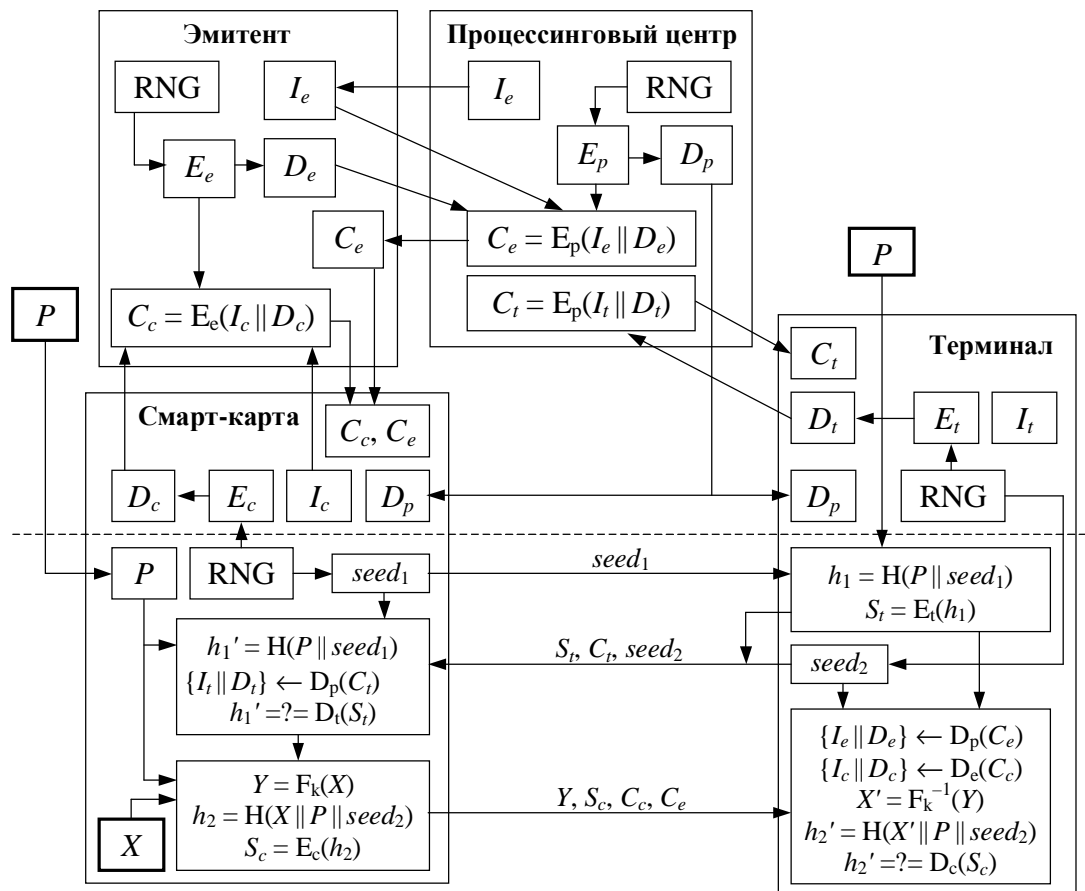


Рис. 4. Схема динамической аутентификации на основе смарт-карт, поддерживающих ЦП

Процедура аутентификации карты в терминале базируется на трехэтапном протоколе:

1. Карта пользователя формирует случайный вектор  $seed_1$  и передаёт его терминалу.
2. Терминал запрашивает ПИН-код владельца карты, объединяет его с полученным вектором  $seed_1$  и вычисляет цифровую подпись  $S_t$  от хеш-функции объединённого значения  $h_1$  на собственном секретном ключе  $E_t$ .
3. Терминал формирует случайный вектор  $seed_2$  и вместе с рассчитанной цифровой подписью  $S_t$  и сертификатом собственного открытого ключа  $C_t$ , отправляет карте пользователя.
4. Карта пользователя извлекает из сертификата  $C_t$  открытый ключ терминала  $D_t$  и, в случае его целостности, проверяет подпись  $S_t$ , сформированную терминалом. Если подпись верна, то карта «считает» терминал подлинным и переходит к следующему этапу

аутентификации, в противном случае процедура аутентификации прерывается.

5. Карта пользователя объединяет полученный от терминала вектор  $seed_2$  с хранящимися в ней данными пользователя  $X$  и его ПИН-кодом  $P$  и вычисляет цифровую подпись  $S_c$  от хеш-функции объединённого значения  $h_2$  на собственном секретном ключе  $E_c$ .
6. Рассчитанная цифровая подпись  $S_c$  вместе с сертификатами открытых ключей карты  $C_c$  и эмитента  $C_e$ , а также данными пользователя  $X$  передаётся терминалу (данные  $X$  передаются в зашифрованном виде  $Y$ , для шифрования может использоваться либо симметричный алгоритм  $F$  и ключ  $k$  выработанный по схеме класса Диффи-Хеллмана либо может использоваться направленное шифрование).
7. Терминал извлекает из полученных сертификатов вначале открытый ключ эмитента, а затем открытый ключ карты. Если оба сертификата целостны, то терминал расшифровывает полученные данные  $X$  и проверяет цифровую подпись карты  $S_c$ . Если подпись верна, то терминал «считает», карту подлинной и переходит к выполнению транзакции, в противном случае процедура аутентификации прерывается.

#### *Достоинства:*

1. Невозможность (высокая технологическая сложность) создания дубликата карты.
2. Защита пользователя от злоупотреблений со стороны персонала, обслуживающего терминальное оборудование.
3. Защита пользователя от злоупотреблений со стороны сотрудников банка.
4. Возможность арбитража в случае конфликтных ситуаций.

#### *Недостатки:*

1. Необходимость применения в смарт-картах специализированных (сравнительно дорогих) чипов.
2. ПИН-код попадает в карту через терминал, который может быть «модифицирован» злоумышленником. Кроме того, вся управляющая информация необходимая для выполнения транзакции вводится и отображается посредством терминалом, а значит может быть фальсифицирована перед передачей на карточку. Данный недостаток характерен для всех схем аутентификации на смарт-картах.

Все рассмотренные карточные технологии аутентификации могут быть реализованы как на основе контактных смарт-карт, так и на основе

безконтактных. При этом последний вариант более предпочтителен, т.к. снижает износ карточки – т.е. способствует увеличению среднего срока её службы. Кроме того, использование технологий безконтактных коммуникаций открывает дополнительные перспективы повышения безопасности. Рассмотрим их подробнее.

## **7. ИСПОЛЬЗОВАНИЕ NFC-МОБИЛЬНЫХ ТЕРМИНАЛОВ**

Последний из рассмотренных недостатков является «неизлечимым пороком» карточных платёжных систем, т.к. в конечном счёте пользователь (владелец карточки) всё равно должен «доверять» терминалу. Этот недостаток может быть устранён только в случае возможности управления смарт-картой с «персонального (личного) терминала» пользователя, т.е. такой терминал должен быть оснащён устройством ввода (желательно клавиатурой) и устройством отображения. Естественно, что такое требование практически не реализуемо для смарт-карт. Однако это требование автоматически удовлетворится при использовании в качестве «смарт-карты» (средства идентификации и аутентификации) мобильного телефона, смарт-фона или PDA, оснащённого средствами Near Field Communication (NFC). В этом случае ПИН-код а также вся информация, необходимая для инициализации транзакции, попадает непосредственно в *персональный* мобильный терминал и не может быть скомпрометирована или модифицирована. Более того, отсутствие электрического контакта между терминалом и устройством аутентификации повышает защищённость последнего, т.к. карта не может быть повреждена воздействиями не штатных напряжений или другими нарушениями в интерфейсе точки доступа.

Для построения надёжного протокола (взаимной) динамической аутентификации может использоваться последняя рассмотренная схема (рис. 4). Единственным отличием от указанной схемы будет отсутствие необходимости использовать ПИН-код для выполнения первых двух шагов аутентификации, т.к. проверка ПИН-кода выполняется ещё на этапе включения (либо инициализации соответствующей функции) мобильного терминала.

## **8. ВЫВОДЫ**

Как видно из рассмотренного материала, единственной схемой позволяющей защитить не

только банк от злоупотреблений со стороны пользователя системы, но и пользователя от угроз злоупотребления со стороны, как обслуживающего персонала, так и сотрудников банка, является *асимметричная динамическая аутентификация с «самостоятельным» формированием секретных ключей карты*. Все остальные рассмотренные схемы предполагают наличие в банке всей информации, необходимой для корректной аутентификации любой транзакции со стороны клиента. Т.е. такая система позволяет защитить только интересы банка от злоупотреблений со стороны клиента, однако не предоставляет защиты для клиента, от злоумышленных действий со стороны банка. При этом целью злоумышленных действий в адрес клиента могут быть как хищение средств, так и компрометация его имени. Этот недостаток особенно существенен для крупных клиентов, где стоимость наносимого ущерба «окупает» «накладные расходы».

Особенного внимания заслуживает возможность использования персональных NFC-терминалов [4] для выполнения «абсолютно защищённых» транзакций, т.к. в этом случае клиент платёжной системы (в общем случае абонент любой системы аутентификации) максимально защищён от злоупотреблений со стороны обслуживающего персонала системы. В случае использования персональных NFC-терминалов необходимый уровень доверия со стороны пользователя к самой системе минимален и единственным доверенным субъектом системы является процессинговый центр, формирующий сертификаты второго уровня. Кроме того, интеграция функций идентификации и аутентификации личности, а также функций электронной коммерции в одном мобильном телефоне (смарт-фоне) или PDA, оснащённом функцией NFC-доступа, значительно упрощает и повышает удобство выполнения различных платёжных операций конечным потребителем. Это связано, в первую очередь, с возможностью выполнения любых платёжных операций и операций идентификации личности с одного устройства, т.е. отсутствует

необходимость носить с собой множество платёжных карт и удостоверений для различных платёжных систем и систем разграничения доступа, и соответственно запоминать множество различных ПИН-кодов или паролей. *Повышение удобства и безопасности использования систем электронных платежей (и идентификации личности) за счёт совмещения указанных функций в одном устройстве позволяет значительно повысить количество потребителей соответствующих услуг.*

На сегодняшний день на рынке доступны все необходимые аппаратные компоненты, необходимые для реализации рассмотренных систем «высокой безопасности». Однако наблюдается определённый «пробел» в области законченных систем, удовлетворяющих требованию «максимальной защищённости пользователя от самой системы», поэтому реализация подобных систем, сегодня является особенно перспективным направлением.

Основным достоинством последней из рассмотренных схем является возможность рассмотрения в суде электронных документов подкреплённых цифровой подписью (в государствах законодательно закрепивших юридическую силу электронных документов и силу цифровой подписи).

## 9. ЛИТЕРАТУРА

1. Wolfgang Rankl, Wolfgang Effing. Smart Card Handbook. Hardcover 2 Ed edition. John Wiley & Sons, 2000.
2. FIPS PUB 201, Federal Information Processing Standards Publication. Personal Identity Verification (PIV) of Federal Employees and Contractors, 2005.  
[http://www.smartcardalliance.org/pdf/industry\\_info/FIPS\\_201\\_022505.pdf](http://www.smartcardalliance.org/pdf/industry_info/FIPS_201_022505.pdf)
3. Government Smart Card Handbook. U.S. General Services Administration, 2004.  
[http://www.smartcardalliance.org/pdf/industry\\_info/smartcardhandbook.pdf](http://www.smartcardalliance.org/pdf/industry_info/smartcardhandbook.pdf)
4. NFC Forum. <http://www.nfc-forum.org/home>