



## Лучшие практики Visa по шифрованию полей данных, версия 1.0

### От точки продаж до эквайера

#### Цели безопасности

1. Ограничить циркуляцию данных о держателях карт и критичных аутентификационных данных в открытом виде только точками шифрования и расшифрования.
2. Использовать надежные решения по управлению ключами, соответствующие международным и/или региональным стандартам.
3. Использовать длины ключей и криптографические алгоритмы, соответствующие международным и/или региональным стандартам.
4. Защитить устройства, выполняющие криптографические операции, от физической и логической компрометации.
5. Для бизнес-процессов, использовать дополнительную учетную запись или идентификатор транзакции, которые не используют PAN после авторизации. Например, при выполнении повторяющихся платежных операций, поддержки программ лояльности клиента или управления инцидентами мошенничества.

#### Среда применимости

- *Лучшие практики Visa по шифрованию полей данных* имеют отношение к системам, выполняющим эквайринговые операции в таких местах, как:
  - Платежные терминалы
  - Точки продаж торгово-сервисных предприятий
  - Корпоративные серверы
  - Корпоративные системы агрегирования транзакций
  - Платежные шлюзы
  - Процессинговые системы
  - Эквайеры
- Данные о держателях карт включают в себя: PAN, имя держателя карты и срок окончания действия карты.
- Критичные аутентификационные данные включают в себя, но не ограничиваются следующими: полное содержимое магнитной дорожки, дорожка 1 (track 1), дорожка 2 (track 2), проверочное значение карты (CVV), CVV2, проверочное значение PIN (PVV) и PIN/PIN block . Критичные аутентификационные данные не могут быть использованы ни для каких целей, кроме как для авторизации транзакции.

## Лучшие практики

Ниже представлены лучшие практики по шифрованию полей данных для защиты данных о держателях карт и критических аутентификационных данных:

Цели безопасности	Рекомендации
<p>Ограничить циркуляцию данных о держателях карт и критичных аутентификационных данных в открытом виде только точками шифрования и расшифрования.</p>	<ol style="list-style-type: none"> <li>1. Данные о держателях карт и критичные аутентификационные данные должны быть доступны в открытом виде только в точках шифрования и расшифрования.</li> <li>2. Все данные о держателях карт и критичные аутентификационные данные должны шифроваться только алгоритмами, одобренными комитетом ANSI X9 или ISO (например, AES, TDES).</li> <li>3. Все данные о держателях карт и критичные аутентификационные данные должны быть зашифрованы, кроме:               <ul style="list-style-type: none"> <li>○ Первые шесть цифр PAN могут оставаться в открытом виде для маршрутизации в процессе авторизации.</li> <li>○ Первые шесть и последние четыре цифры PAN могут выводиться на экран платежного терминала и/или распечатываться на чеке, в отчетах об оплате, использоваться для выбора счета, и т.д. (эта рекомендация не заменяет более строгих правил и регламентов, которые имеются в организациях, касательно отображения данных о держателях карт).</li> </ul> </li> <li>4. Критичные аутентификационные данные не должны сохраняться после авторизации, даже в зашифрованном виде (согласно PCI DSS).</li> </ol>
<p>Использовать надежные решения по управлению ключами, соответствующие международным и/или региональным стандартам.</p>	<ol style="list-style-type: none"> <li>5. Управление ключами должно осуществляться в соответствии со стандартами ANS X9.24 (все части) / ISO 11568 (все части) или их аналогами, с использованием защищенных криптографических устройств (Secure Cryptographic Devices, SCD), таких как PED, HSM, и т.п., как определено в стандартах ANS X9.97 (все части) / ISO 13491 (все части) или их аналогах.</li> <li>6. Все ключи и их компоненты должны генерироваться с использованием одобренных процедур случайного или псевдослучайного подбора, например, NIST SP 800-22.</li> <li>7. Документация, описывающая процесс установки и функционирования системы управления ключами, должна быть доступной по запросу для ее оценки.</li> <li>8. Перевозка или передача ключей по каналам связи должна быть защищена. Например, используя метод распространения ключей, описанный в <i>X9/TR-34 Interoperable Method for Distribution of Symmetric Keys Using Asymmetric Techniques, Part 1—Using Factoring-Based Public Key Cryptography Unilateral Key Transport</i> или эквивалентный метод.               <ul style="list-style-type: none"> <li>○ Если используется дистанционное распространение ключей, должна осуществляться обоюдная аутентификация устройств отправки и получения.</li> </ul> </li> <li>9. Ключи, используемые в процессе шифрования поля данных, должны:               <ul style="list-style-type: none"> <li>○ Быть уникальными для каждого устройства.</li> </ul> </li> </ol>

	<ul style="list-style-type: none"> <li>○ Использоваться только для шифрования данных о держателях карт и критичных аутентификационных данных, и не должны использоваться для других целей.</li> <li>○ Ключи, используемые для шифрования PIN, не могут быть использованы для шифрования поля данных (в соответствии с PCI PIN Security Requirements).</li> </ul>												
<p>Использовать длины ключей и криптографические алгоритмы, соответствующие международным и/или региональным стандартам.</p>	<p>10. Ключи шифрования должны обладать стойкостью, эквивалентной стойкости, как минимум, 112-битного ключа. В таблице представлены эквивалентные стойкости часто используемых алгоритмов.</p> <table border="1" data-bbox="703 674 1195 850"> <thead> <tr> <th>Алгоритм</th> <th>Длина в битах</th> </tr> </thead> <tbody> <tr> <td>TDES</td> <td>112<sup>1</sup></td> </tr> <tr> <td>AES</td> <td>128<sup>2</sup></td> </tr> <tr> <td>RSA</td> <td>2048</td> </tr> <tr> <td>ECC</td> <td>224</td> </tr> <tr> <td>SHA</td> <td>224</td> </tr> </tbody> </table> <p>Для более подробной информации касательно эквивалентной стойкости, обратитесь к <i>ISO TR-147442 Recommendations on Cryptographic Algorithms and their Use – Technical Report</i>.</p> <p>11. Любые методы, используемые для производства шифртекста такой же длины и типа данных, как и у открытого текста, должны пройти оценку как минимум одной независимой организации по оценке безопасности. Эти методы должны внедряться в соответствии с рекомендациями, выданными при выполнении вышеупомянутой оценки, включая все рекомендации по сопутствующему управлению ключами.</p>	Алгоритм	Длина в битах	TDES	112 <sup>1</sup>	AES	128 <sup>2</sup>	RSA	2048	ECC	224	SHA	224
Алгоритм	Длина в битах												
TDES	112 <sup>1</sup>												
AES	128 <sup>2</sup>												
RSA	2048												
ECC	224												
SHA	224												
<p>Защитить устройства, выполняющие криптографические операции, от физической и логической компрометации.</p>	<p>12. Устройства, выполняющие криптографические операции, должны подвергаться независимой оценке, для гарантии того, что их комплектующие и программное обеспечение устойчивы к атакам.</p> <p>13. Симметричные и закрытые ключи должны быть защищены от физической и логической компрометации. Открытые ключи должны быть защищены от подмены, а их целостность и достоверность должны быть гарантированы.</p>												
<p>Для бизнес-процессов, использовать дополнительную учетную запись или идентификатор транзакции, которые не</p>	<p>14. Если какие-либо данные о держателях карт (например, PAN) необходимы после авторизации, то вместо них следует использовать одноразовый или многократный идентификатор транзакции.</p> <ul style="list-style-type: none"> <li>○ Предпочтителен одноразовый идентификатор транзакции. <ul style="list-style-type: none"> <li>▪ Допустимые методы получения одноразового идентификатора транзакции включают хэширование PAN с уникальным для транзакции значением привязки, шифрование PAN одобренным алгоритмом с использованием уникального для транзакции ключа,</li> </ul> </li> </ul>												

<p>используют PAN после авторизации. Например, при выполнении повторяющихся платежных операций, поддержки программ лояльности клиента или управления инцидентами мошенничества.</p>	<p>или эквивалентным. Одноразовый идентификатор транзакции может быть получен другими методами, которые обеспечивают уникальность идентификатора для каждой транзакции, при этом данные о держателях карт не должны быть читаемы.</p> <ul style="list-style-type: none"> <li>○ Многоразовый идентификатор транзакции может использоваться, если существует необходимость обеспечения взаимосвязи номера счета с несколькими транзакциями. <ul style="list-style-type: none"> <li>▪ Допустимые методы получения многоразового идентификатора транзакции включают хеширование данных о держателях карт, используя фиксированное (но разное для каждого торгового-сервисного предприятия) значение привязки или эквивалентное.</li> </ul> </li> </ul> <p><b>ПРИМЕЧАНИЕ:</b> Независимо от того, какой тип идентификатора транзакции используется (одноразовый или многоразовый), если применяются значения привязки, то их длина должна быть минимум 32 бита, они должны находиться в тайне и быть должным образом защищены.</p>
---	---

---

<sup>1</sup> В целях данных лучших практик, два ключа TDES (112 бит) не должны обрабатывать более 1 миллиона транзакций. В случаях, когда количество транзакций, потенциально обрабатываемых ключом 112 бит TDES, намного превышает 1 миллион, следует использовать ключи TDES (168 бит) или AES. Схемы управления ключами, которые ограничивают количество транзакций для одного ключа, например «производный уникальный транзакционный ключ» (Derived Unique Key Per Transaction, DUKPT), могут использоваться для обеспечения того, что каждый отдельный ключ используется строго ограниченное количество раз.

<sup>2</sup> Минимальное количество бит в ключе, которые можно использовать с AES, составляет 128 бит. Данный ключ более стоек, чем это необходимо, но если используется AES, это наименьший из доступных ключей (более длинные ключи могут быть использованы по желанию).

---