# Ключ к безопасной мобильной подписи: от защиты ключа на пароле к двусторонней подписи

Е.К. Алексеев, Л.Р. Ахметзянова, Л.О. Никифорова, С.В. Смышляев

***Аннотация*— На сегодняшний день массовое применение криптографических механизмов неразрывно связано с использованием мобильных устройств. При этом возникает проблема их низкого уровня защищенности, как в организационном плане, так и в инженерно-техническом. Это требует от применяемых аппаратно-программных решений защищенности не только в стандартных моделях нарушителя, но и в расширенных, предполагающих, что часть базовых требований по безопасной эксплуатации были нарушены, что привело к компрометации устройства или пароля. В настоящей работе проводится анализ защищенности пяти распространенных классов решений для работы с электронной подписью в нескольких распространенных расширенных моделях нарушителя. Отдельно исследуется вопрос необходимости наличия доверия к дополнительной стороне взаимодействия.**

***Ключевые слова*—электронная подпись, мобильные устройства, двусторонняя подпись.**

## I. Введение

На сегодняшний день наиболее массово используемыми вычислительными машинами являются мобильные телефоны или смартфоны. Это приводит к тому, что массовое применение криптографических механизмов связывается именно с такими устройствами. При этом массовость неизбежно означает низкий уровень организационной и инженерно-технической защищенности на стороне пользователя. Наиболее частыми следствиями этого являются кража устройств, компрометация пароля и установка на устройство пользователя вредоносного программного обеспечения (ВПО). Это приводит к необходимости оценки защищенности применяемых решений не только в стандартных моделях нарушителя, но и в расширенных. Такие модели предполагают, что какие-то негативные для пользователя ситуации уже реализовались. Примеры такого анализа можно найти в работах [1,2].

В настоящей работе исследуется защищенность пяти классов программно-аппаратных решений для работы с электронной подписью. Эти решения анализируются в условиях, когда нарушитель может реализовывать ряд априори негативных для пользователя ситуаций, таких как кража его мобильного устройства.

Часть результатов, изложенных в настоящей работе, была представлена на симпозиуме CTCrypt в 2024 году [3].

Алексеев Евгений Константинович, ООО "КРИПТО-ПРО", email:alekseev@cryptopro.ru
Ахметзянова Лилия Руслановна, ООО "КРИПТО-ПРО", email:lah@cryptopro.ru
Никифорова Лидия Олеговна, ООО "КРИПТО-ПРО", email:nikiforova@cryptopro.ru
Смышляев Станислав Витальевич, ООО "КРИПТО-ПРО", email:svs@cryptopro.ru

## II. Рассматриваемые решения и свойства

В настоящей работе рассмотрим классы программно-аппаратных решений для формирования и проверки электронной подписи, предполагающие мобильность устройства пользователя и отличающиеся друг от друга по месту хранения ключа формирования электронной подписи и по методу его защиты. Далее перечислим рассматриваемые в настоящей работе классы решений (далее, для удобства, будем иногда называть их просто «решения»), приведя для каждого из них краткое название, а также описание порядка его функционирования.

- **"Смартфон"**: ключ формирования подписи хранится на мобильном устройстве пользователя в зашифрованном виде. Ключ защиты ключа подписи вырабатывается из пароля, который запоминается пользователем и нигде не хранится.
- **"Смарт-карта"**: решения данного класса предполагают, что ключ формирования электронной подписи хранится на отчуждаемом носителе (смарт-карте), с которым взаимодействует смартфон пользователя. Носитель предоставляет устройству возможность использовать ключ в случае ввода пользователем правильного пароля.
- **"Сервер"**: ключ хранится на сервере, защита доступа к ключу осуществляется с помощью пароля и мобильного устройства. Данный класс решений часто называют "облачной подписью".
- **"Смартфон под защитой сервера"**: ключ хранится на мобильном устройстве пользователя в зашифрованном виде, но, в отличие от решений класса "Смартфон", шифрование осуществляется на ключе, каждый раз предоставляемом сервером по запросу клиента. Контроль за возможностью предоставления ключа осуществляется с помощью пароля.
- **"Смартфон и сервер"** ключ хранится в "распределенном" между клиентской и

серверной компонентой виде. Под этим подразумевается, что ни в какой момент времени он не появляется ни на стороне клиента, ни на стороне сервера, а подпись может быть сформирована только в результате взаимодействия между обеими сторонами. Допустимость взаимодействия клиента с сервером контролируется с помощью пароля. Криптографические схемы, используемые в таком случае, обычно называются двусторонними подписями, они рассматривались, например, в работах [4,5,6].

Перечисленные решения будут сравниваться с точки зрения обеспечения ими защиты при наступлении определенных событий, связанных с компрометацией участников взаимодействия.

Начнем с классификации таких событий. Далее будут рассматриваться:

- **Кража устройств**. В данном случае рассматривается кража устройства пользователя, а именно, смартфона и/или смарт-карты. Предполагается, что кража является обнаружимым событием.
- **Кража устройств и пароля**. В сравнении с предыдущим случаем в данном случае помимо кражи самого устройства пользователя нарушитель также может получить его пароль, например, вследствие его небезопасного хранения или использования.
- **ВПО на устройстве**. В данном случае предполагается, что на устройстве пользователя установлено специальное программное обеспечение нарушителя, имеющее доступ на чтение и запись к оперативной памяти устройства во время его использования пользователем.
- **Компрометация сервера**. В данном случае предполагается, что нарушитель фактически заменяет собой сервер и имеет доступ ко всей информации, хранящейся на сервере.

Защищённость решений будет анализироваться на предмет возможности возникновения следующих ситуаций, которые могут привести к определенному ущербу на практике (ситуации представлены в порядке убывания возможного практического ущерба):

- Нарушитель смог сформировать поддельную подпись для некоторого документа, при этом пользователь не имеет возможности обнаружить факт создания такой подписи (**подделка без обнаружения факта**). В данной ситуации пользователь не догадывается о необходимости предпринять какие-либо меры для предотвращения дальнейшего создания и использования подделок.
- Нарушитель смог сформировать поддельную подпись для некоторого документа, но пользователь имеет возможность обнаружить факт создания такой подписи (**подделка с обнаружением факта**). В данной ситуации пользователь может успеть отозвать соответствующий сертификат проверки подписи для предотвращения создания нарушителем подписей для других документов.
- Нарушитель смог сформировать поддельную подпись для некоторого документа, но пользователь имеет возможность обнаружить не только факт создания такой подписи, но и узнать, для какого документа данная подпись была сформирована (**подделка с обнаружением документа**). В данной ситуации пользователь имеет возможность понять, для каких целей будет использоваться подделка и предпринять соответствующие меры для минимизации ущерба (например, лично обратиться в соответствующую организацию, где будет применяться поддельная подпись, с запросом на блокирование любых действий с его стороны).

Далее при рассмотрении каждого решения для каждого сценария компрометации будем определять ситуацию с наибольшим ущербом, которая может быть реализована.

## III. "Смартфон"

Решения данного класса являются наиболее простыми в использовании, но наименее защищенными из всех рассматриваемых в настоящей работе. При рассмотрении решений данного класса под устройством пользователя понимается смартфон.

Решение «Смартфон» предполагает хранение ключа подписи на смартфоне под защитой ключа, который вырабатывается из пароля, запоминаемого пользователем.

В случае кражи смартфона нарушитель, в силу зашифрования ключа формирования подписи, по сути, на пароле, получает доступ к этому ключу. Такой вывод справедлив с учетом базового предположения о том, что нарушитель имеет вычислительные возможности, достаточные для перебора низкоэнтропийных секретов. Однако кражу смартфона можно вовремя обнаружить и отозвать сертификат. Таким образом, в случае кражи устройства может быть реализована подделка с обнаружением факта.

Аналогично предыдущему случаю, в случае кражи устройства и пароля так же может быть реализована подделка с обнаружением факта.

В случае наличия ВПО на устройстве пользователя нарушитель может получить доступ к ключу подписи в момент, когда он появляется в оперативной памяти устройства при подписании. После получения данного ключа нарушитель может уже подписывать любые документы, и пользователь не сможет вовремя это обнаружить. Таким образом, в случае ВПО на устройстве может быть реализована подделка без обнаружения факта.

Случай компрометации сервера не является актуальным для рассмотрения, так как сервер не используется в данном решении.

## IV. "Смарт-карта"

Решения данного класса используются в случае наличия отчуждаемых носителей, на которых хранится

ключ подписи и которые защищены с помощью организационно-технических мер. Так, архитектура ряда смарт-карт последнего поколения предполагает, что ключ подписи никогда не покидает устройство и все операции с ним выполняются самой смарт-картой (см., например, [7]). При рассмотрении решений данного класса под устройством пользователя понимается смартфон и смарт-карта пользователя.

Для аутентификации обращений к функции подписания используется пароль, запоминаемый пользователем. Данный пароль вводится владельцем карты в смартфон, далее с помощью данного пароля смартфон аутентифицируется перед смарт-картой. Смарт-карта в свою очередь стандартно применяет механизмы для защиты от онлайн-перебора пароля (например, счетчики попыток ввода пароля).

В случае кражи только смарт-карты нарушитель не может получить доступ к ключу без знания пароля. Кража смартфона является бессмысленной, так как ключ формирования подписи на нем не хранится. Таким образом, в случае кражи устройств ни одна из ситуаций, приводящих к какому-либо ущербу, не может быть реализована.

В случае компрометации и пароля, и смарт-карты нарушитель получает полный контроль над ключом подписи и может подписывать любые сообщения. Однако кражу смарт-карты можно вовремя обнаружить и отозвать сертификат. Таким образом, в случае кражи устройства и пароля может быть реализована подделка с обнаружением факта.

В случае наличия ВПО на смартфоне, оно может передавать неправильные документы для подписи, однако пользователь имеет возможность путем проверки полученной подписи обнаружить, что подпись не является корректной для целевого документа. Возможность наличия ВПО на смарт-карте не рассматривается. Таким образом, в случае ВПО на смартфоне может быть реализована подделка с обнаружением факта.

Случай компрометации сервера не является актуальным для рассмотрения, так как сервер не используется в данном решении.

## V. "Сервер"

Решения данного класса зачастую предполагают использование на стороне сервера специализированного защищенного вычислителя, предназначенного для централизованного хранения ключей подписи и имеющего достаточно высокий уровень программно-аппаратной и организационной защиты (обычно такие модули называются HSM – Hardware Security Module). При рассмотрении решений данного класса под устройством пользователя понимается смартфон.

В решениях данного класса для аутентификации перед сервером пользователь использует запоминаемый пароль и высокоэнтропийный секрет (ключ), который хранится на смартфоне. Для формирования подписи пользователь обращается к серверу, аутентифицируется и передает документ для подписания. Сервер использует методы защиты от онлайн-перебора пароля при аутентификации пользователя.

В случае кражи устройства пользователя нарушитель получает доступ только к секрету устройства. В силу того, что пароль пользователя нарушителю не известен и он не может подобрать его в режиме онлайн, нарушитель не сможет аутентифицироваться перед сервером и, как следствие, не сможет сформировать ни одной подписи от имени пользователя. Таким образом, в случае кражи устройства ни одна из ситуаций, приводящих к какому-либо ущербу, не может быть реализована.

В случае кражи устройства пользователя и его пароля нарушитель имеет возможность взаимодействовать с сервером от имени пользователя и инициировать подписание произвольных документов с использованием его ключа подписи. Для формирования каждой новой подписи нарушитель должен отправлять на сервер документ для подписания, при этом сервер фиксирует факт подписания документа и сам подписываемый документ. Таким образом, в случае кражи устройства и пароля может быть реализована подделка с обнаружением документа.

Для решений данного класса возможности нарушителя в случае наличия ВПО на смартфоне совпадают с возможностями нарушителя в случае кражи устройства и пароля. Таким образом, в данном случае может быть реализована подделка с обнаружением документа.

В случае компрометации сервера нарушитель получает доступ к ключу подписи пользователя. Это означает, что нарушитель имеет возможность бесконтрольно использовать ключ подписи пользователя. Таким образом, в случае компрометации сервера может быть реализована подделка без обнаружения факта.

## VI. "Смартфон под защитой сервера"

Идеей, лежащей в основе решений данного класса, является защита ключа подписи, хранящегося на устройстве пользователя, с помощью высокоэнтропийного ключа, который хранится на сервере. Доступ к ключу защиты ключа подписи для пользователя осуществляется после аутентификации пользователя на сервере с помощью пароля. Как и в других классах решений, сервер использует методы защиты от онлайн-перебора пароля. При рассмотрении решений данного класса под устройством пользователя понимается смартфон пользователя.

В случае кражи устройства пользователя, в отличие от решения "Смартфон", нарушитель уже не может получить доступ к ключу подписи путем перебора пароля. Действительно, ключ подписи защищен уже на неперебираемом секрете, доступ к которому можно получить только в результате успешной аутентификации. Таким образом, в случае кражи устройства ни одна из ситуаций, приводящих к какому-либо ущербу, не может быть реализована.

В случае кражи устройства и пароля пользователя нарушителю необходимо провести одно взаимодействие с сервером, в результате которого он получит ключ защиты, расшифрует ключ подписи и далее сможет пользоваться им без взаимодействия с сервером. При этом, так как нарушителю нужно осуществить хотя бы одно взаимодействие с сервером, факт компрометации устройства может быть обнаружен, например, если сервер сообщает о начале операции подписания по дополнительным каналам. Однако обнаружить, какой конкретно документ был подписан нарушителем

пользователь не может. Таким образом, в случае кражи устройства и пароля может быть реализована подделка с обнаружением только факта.

В случае наличия ВПО на устройстве пользователя нарушитель может получить доступ к ключу подписи в момент, когда он появляется в оперативной памяти устройства при подписании. После получения данного ключа нарушитель может подписывать любые документы, и пользователь не может вовремя обнаружить этот факт. Таким образом, в этом случае может быть реализована подделка без обнаружения факта.

В случае компрометации сервера нарушитель не получает доступа к ключу подписи пользователя, так как сервер хранит только секрет, используемый для защиты ключа подписи, но не зависящий от него. Таким образом, в случае компрометации сервера ни одна из ситуаций, приводящих к какому-либо ущербу, не может быть реализована.

## VII. "Смартфон и сервер"

Решения данного класса также предполагают наличие стороннего сервера, который хранит часть ключа подписи пользователя [1,2,3]. В отличие от решения «Смартфон под защитой сервера», данное решение позволяет обеспечить возможность обнаружения подписываемых нарушителем документов в случае даже самого опасного варианта компрометации – наличия ВПО на смартфоне.

В рамках данного решения предполагается, что ключ подписи генерируется распределенным образом: одна доля ключа хранится на смартфоне, другая доля ключа хранится на сервере. Для того, чтобы сформировать подпись пользователь должен обратиться к серверу, аутентифицировать инициирование операции с помощью пароля, передать документ и далее вместе с сервером выполнить распределенный протокол формирования подписи для этого документа. Сервер осуществляет контроль попыток аутентификации с помощью пароля, а также фиксирует в журнале аудита документ, для которого формировалась подпись.

**Таблица 1: Защищенность решений для электронной подписи в условиях частичной компрометации. Здесь зеленый цвет означает, что нарушитель не может осуществить подделку, желтый – возможна подделка подписи с обнаружением документа, оранжевый – возможна подделка подписи с обнаружением факта подделки, красный – возможна подделка подписи без обнаружения факта подделки. Серым обозначены случаи, которые не являются осмысленными.**

| | Кража устройств | Кража устройств и пароля | ВПО на устройстве | Компрометация сервера |
|---|---|---|---|---|
| "Смартфон" | | | | |
| "Смарт-карта" | | | | |
| "Сервер" | | | | |
| "Смартфон под защитой сервера" | | | | |
| "Смартфон и сервер" | | | | |

В случае кражи устройства пользователя нарушитель может получить доступ только к доле ключа подписи, с помощью которой он не может сформировать подпись. Для того, чтобы сформировать подписи ему необходимо угадать пароль для предъявления серверу. Таким образом, в случае кражи устройства ни одна из ситуаций, приводящих к какому-либо ущербу, не может быть реализована.

В случае кражи устройства и пароля пользователя нарушитель может взаимодействовать с сервером от лица пользователя. Однако, сервер фиксирует все операции с ключом, а также подписываемые документы, и может оповещать об этом пользователя по сторонним каналам. Таким образом, в случае кражи устройства и пароля может быть реализована подделка с обнаружением документа.

В случае наличия ВПО на устройстве пользователя ситуация аналогична краже устройства и пароля. Таким образом, в таком случае может быть реализована подделка с обнаружением документа.

В случае компрометации сервера нарушитель получает доступ только к доле ключа подписи пользователя и паролю, с помощью которых нарушитель не может сформировать подпись. Таким образом, в случае компрометации сервера ни одна из ситуаций, приводящих к какому-либо ущербу, не может быть реализована.

## VIII. Заключение

В настоящей работе была проанализирована защищенность пяти классов решений для работы с электронной подписью, распространенных на практике для массового применения. Результаты сравнения кратко приведены в таблице 1. Заметим, что случай компрометации сервера отличается от остальных случаев, в которых проводился анализ. При этом защищенность некоторого класса решений в данном случае означает, что это решение не требует от пользователя доверия к серверу.

Также в заключение отметим, что создание наиболее защищенного решения типа "Смартфон и сервер" стало возможным исключительно благодаря использованию

принципиально нового криптографического механизма – двусторонней подписи. Таким образом, на технологическом уровне возможность реализации электронной подписи в двустороннем (распределенном) варианте становится крайне важным для практической защищенности.

## Библиография


[1] Aranha D., Novaes F., Takahashi A., Tibouchi M., Yarom Y. "LadderLeak: Breaking ECDSA with Less than One Bit of Nonce Leakage". CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security. pp. 225-242. 2020.

[2] Fouque P.A., Tibouchi M., Zapalowicz J.C. (2013). "Recovering Private Keys Generated with Weak PRNGs". In: Stam, M. (eds) Cryptography and Coding. IMACC 2013. Lecture Notes in Computer Science, vol 8308. Springer, Berlin, Heidelberg.

[3] Алексеев Е.К., Никифорова Л.О. "Электронная подпись в условиях массового применения", CTCrypt 2024.

[4] Алексеев Е.К., Ахметзянова Л.Р., Бабуева А.А., Никифорова Л.О., Смышляев С.В. "Двусторонняя схема подписи ГОСТ", Матем. вопр. криптогр., 15:2 (2024), 7–28. https://doi.org/10.4213/mvk467

[5] Akhmetzyanova L.R., Alekseev E.K., Smyshlyaev S.V., Babueva A.A., Nikiforova L.O. "Two-party signature: how to sign securely using a mobile device", AgileCrypto 2025, https://agilecrypto.biz/en

[6] Lindell Y. "Fast Secure Two-Party ECDSA Signing". J Cryptol 34, 44 (2021).

[7] Агафьин С.С., Смышляев С.В. "Повышение безопасности доступа к ключам электронной подписи в условиях слабодоверенного окружения". International Journal of Open Information Technologies ISSN: 2307-8162, vol. 9, no. 10, 2021.

# The key to secure mobile signature: from password-based protection to two-party signatures

E.K. Alekseev, L.R. Akhmetzyanova, L.O. Nikiforova, S.V. Smyshlyaev

***Abstract*— Nowadays, the widespread deployment of cryptographic mechanisms is inextricably linked to the use of mobile devices. However, this introduces the problem of their relatively low level of security — both in organizational and technical-engineering aspects. This requires that hardware and software solutions provide protection not only within standard adversary models but also within extended ones, which assume that some of the basic security requirements for safe operation have been violated, resulting in the compromise of the device or the user's password.**

**This paper presents an analysis of the security of five common classes of solutions for electronic signature operations under several representative extended adversary models. Additionally, the study examines the necessity of establishing trust to an additional party involved in the interaction.**

***Keywords*— digital signature, mobile device, two-party signature.**

## REFERENCES

[1] Aranha D., Novaes F., Takahashi A., Tibouchi M., Yarom Y. "LadderLeak: Breaking ECDSA with Less than One Bit of Nonce Leakage". CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security. pp. 225-242. 2020.

[2] Fouque P.A., Tibouchi M., Zapalowicz J.C. (2013). "Recovering Private Keys Generated with Weak PRNGs". In: Stam, M. (eds) Cryptography and Coding. IMACC 2013. Lecture Notes in Computer Science, vol 8308. Springer, Berlin, Heidelberg.

[3] Alekseev E.K., Nikiforova L.O. "Electronic Signature in the Context of Mass Adoption", CTCrypt 2024, (in Russian).

[4] Alekseev E.K., Akhmetzyanova L.R., Babueva A.A., Nikiforova L.O., Smyshlyaev S.V. "Two-party Signature Scheme of GOST", Mathematical Aspects of Cryptography, 15:2 (2024), 7–28., (in Russian).
https://doi.org/10.4213/mvk467

[5] Akhmetzyanova L.R., Alekseev E.K., Smyshlyaev S.V., Babueva A.A., Nikiforova L.O. "Two-party signature: how to sign securely using a mobile device", AgileCrypto 2025, https://agilecrypto.biz/en

[6] Lindell Y. "Fast Secure Two-Party ECDSA Signing". J Cryptol 34, 44 (2021).

[7] Agafyin S.S., Smyshlyaev S.V. "Enhancing the Security of Access to Electronic Signature Keys in a Weakly Trusted Environment", International Journal of Open Information Technologies, ISSN: 2307-8162, vol. 9, no. 1.