Протокольные решения для безопасного формирования электронной подписи в облаке

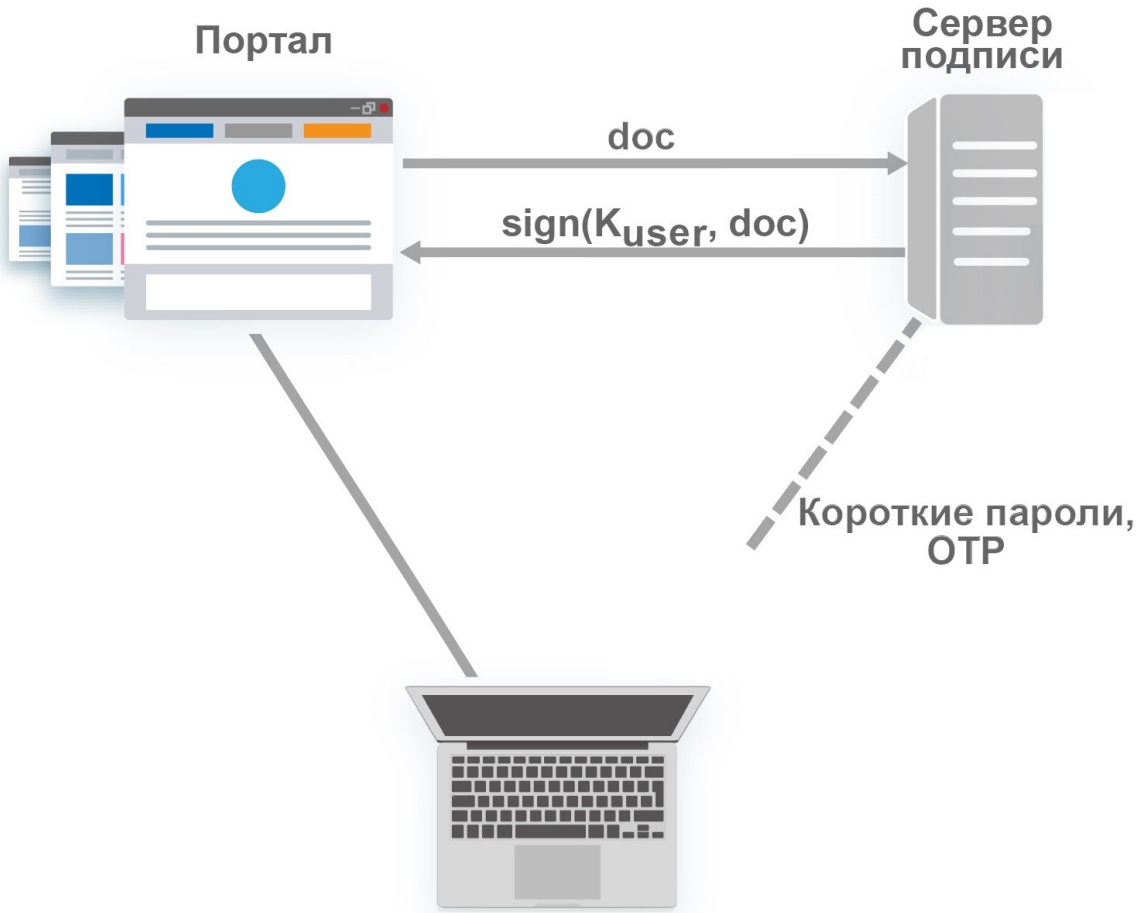
Смышляев Станислав Витальевич, к.ф.-м.н.,
начальник отдела защиты информации

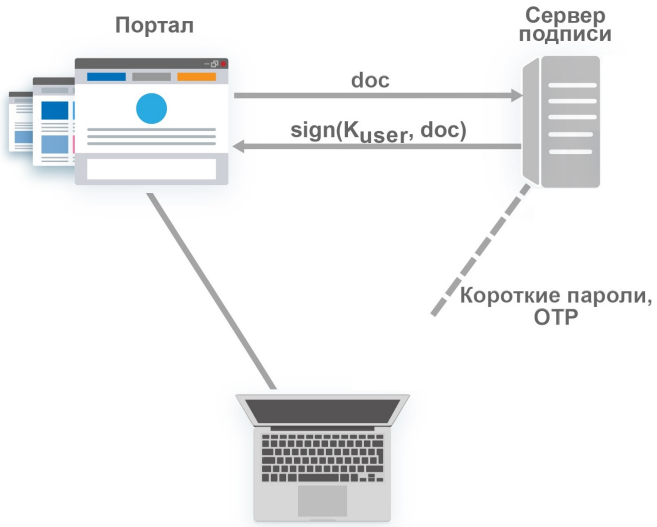
Алексеев Евгений Константинович, к.ф.-м.н.,
ведущий инженер-аналитик

РусКрипто'2016

КРИПТО ПРО

Подпись в облаке: типичный сценарий работы





- Пользователь работает с порталом (сервер СЭД, ДБО, ЭТП).
- На портале происходит формирование документа, который требуется подписать.
- Документ направляется на сервер электронной подписи.
- Одним из согласованных способов [по доверенному каналу] происходит аутентификация операции пользователем.
- Документ подписывается на сервере и направляется на портал.

КРИПТО

Преимущества

- Упрощение процедур обращения с СКЗИ/СЭП.
- Упрощение внедрения форматов подписи (например: формат, упомянутый в 445-ФЗ).
- Упрощение процедур модернизации системы.
- Расширенные возможности аудита.

Задачи

- Минимизация требований к квалификации и орг. мерам.
- Аутентификация операций: доверенная и простая для пользователя работа с системой.
- Простые процедуры доверенной доставки пользовательского ПО для доступа к системе.
- Доверие к хранению ключа.
- Визуализация подписываемых данных перед транзакцией.

КРИПТО ПРО

Аналог: требования CEN

Security Requirements for Trustworthy Systems Supporting Server Signing Европейского Комитета по Стандартизации (CEN)

Требования и рекомендации к построению серверов электронной подписи, позволяющих формировать ЭП, эквивалентную полученной на персональном доверенном защищенном специализированном устройстве (например, криптографическом токене), и, соответственно, эквивалентную собственноручной.

- Уровень 1: аутентификация производится на приложение на пользовательской системе, которое далее само связывается с сервером подписи для формирования автоматизированной подписи.
- Уровень 2, Квалифицированная электронная подпись (QES).

КРИПТО ПРО

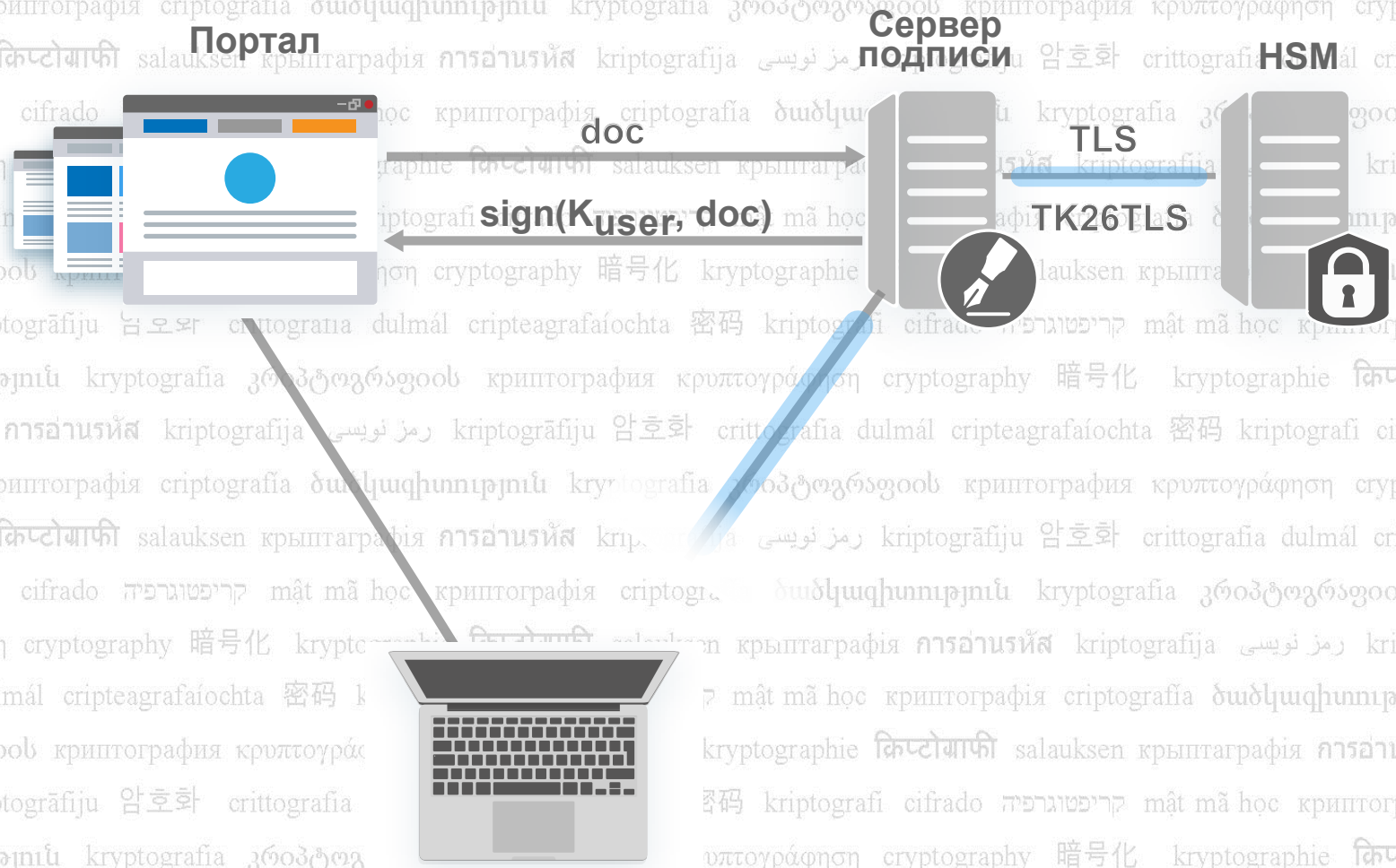
Уровень 2

- Поддержка строгих вариантов аутентификации на сервере подписи, при которых процесс аутентификации пользователя происходит напрямую на сервер подписи.
- Пользовательские ключи подписи для формирования квалифицированной ЭП должны храниться строго в памяти специализированного защищенного устройства (криптографический токен, HSM).
- Аутентификация пользователя на сервере электронной подписи обязана быть как минимум двухфакторной.

Общие требования к безопасности облачной подписи

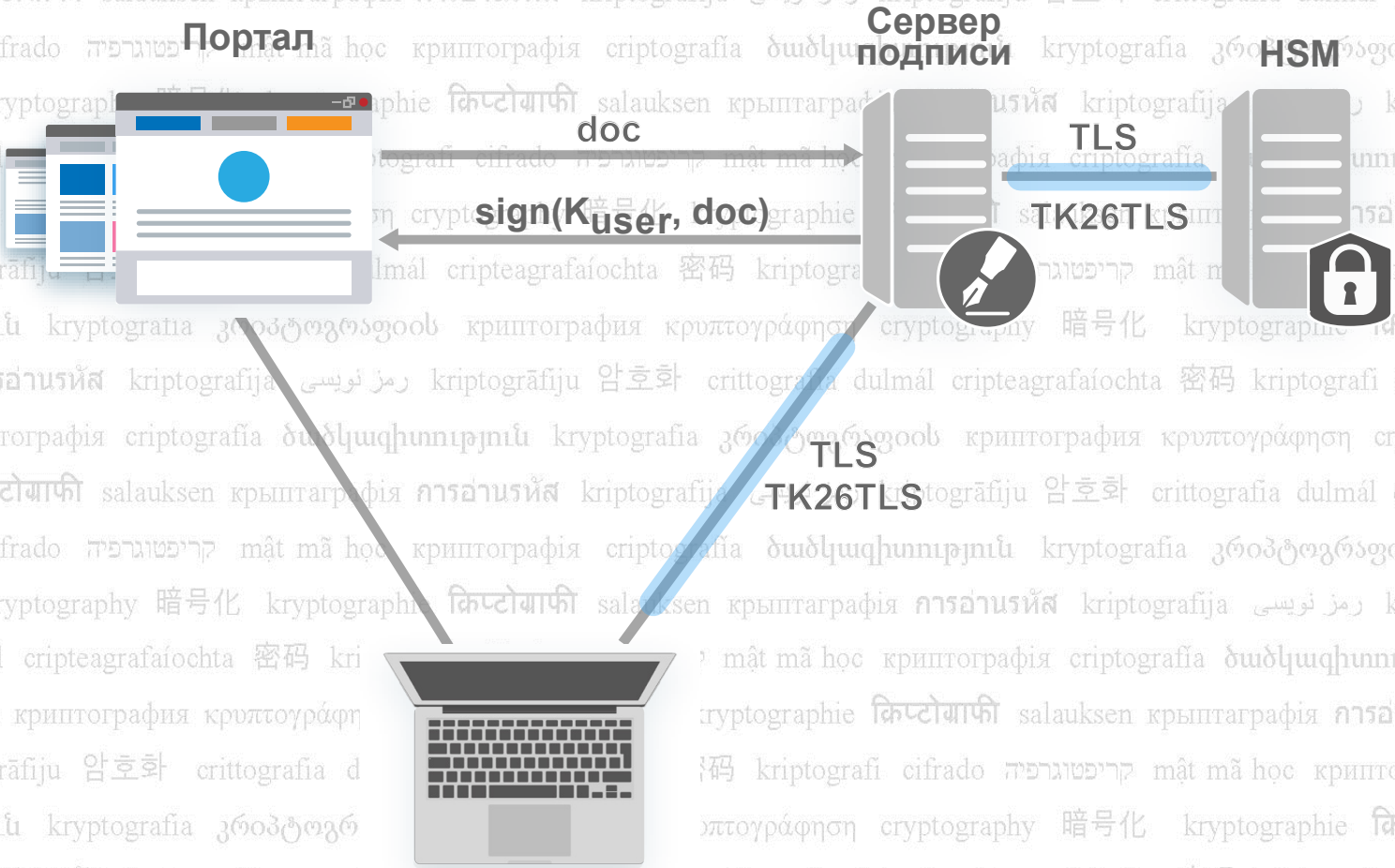
- Требования к СКЗИ/СЭП на стороне сервера в части хранения и использования ключевой информации.
- Надежность механизмов аутентификации пользователей на хранимые ключи.
- Однозначное соответствие между процедурами использования ключа на сервере и операциями пользователя.
- Доверие к клиентским модулям аутентификации операций.

Доверие к хранению ключей и к каналу

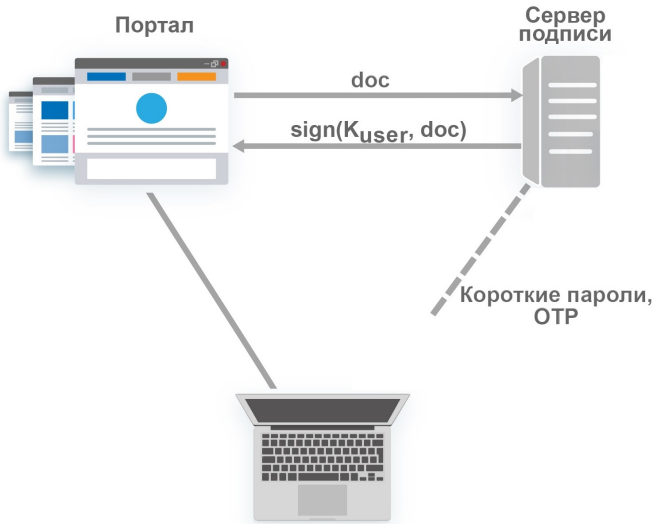


КРИПТО ПРО

Прямолинейный вариант работы с облаком

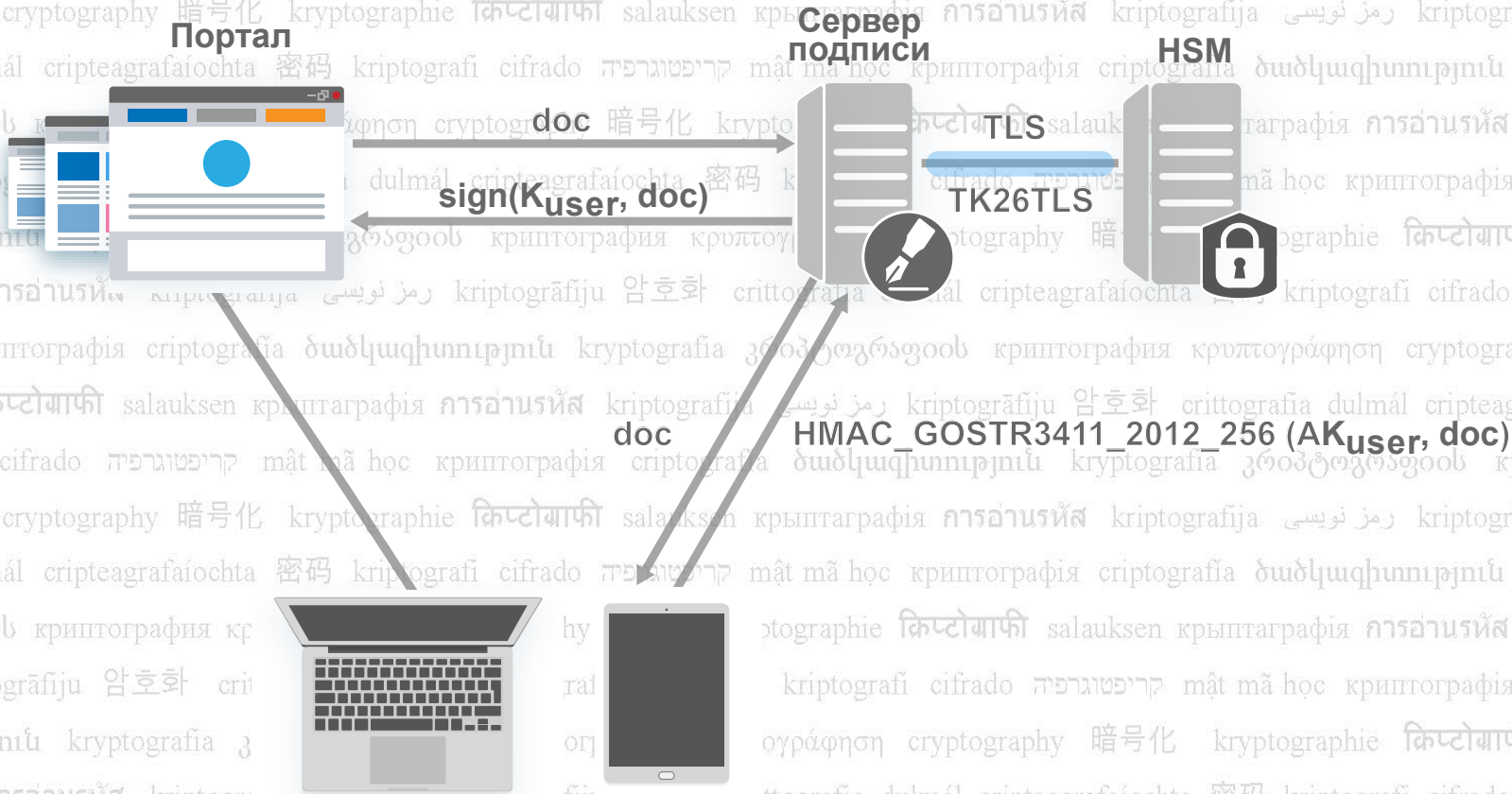


Массово используемые решения



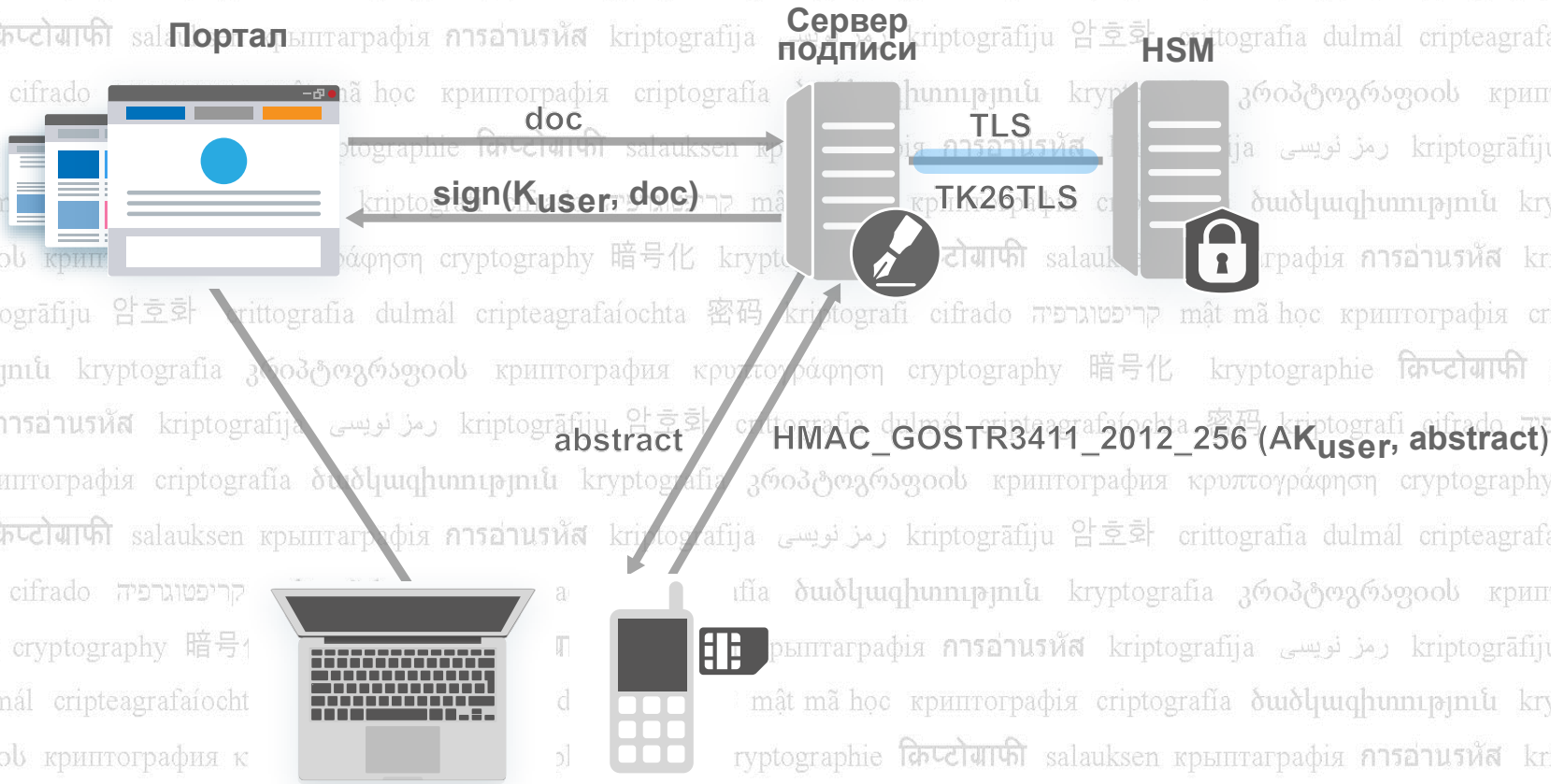
- Короткие и длинные пароли, OTP, внешние сервисы «authentication-as-a-service»...
- Аутентификация пользователя в системе и подтверждение самого факта транзакции.
- Атомарность, ПДСЧ (OTP), атаки на канал, перевыпуск SIM [...] — см. доклад Positive Technologies (Тимур Юнусов).

Аутентификация операций с ключами



Использование SIM-карт для аутентификации на ключ

- Аутентификация операций с использованием HMAC_GOSTR3411_2012_256 в соответствии с Рекомендациями по стандартизации ТК26 «Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012».
- Вычисление HMAC производится от:
  - идентификатор операции;
  - выжимка документа.
- Использование только тех форматов/шаблонов документов, для которых в процессе тематических исследований подтверждено строгое однозначное соответствие информативной части документа выжимке.
- Распределение симметричных ключей аутентификации операций — на основе ключевых деревьев.



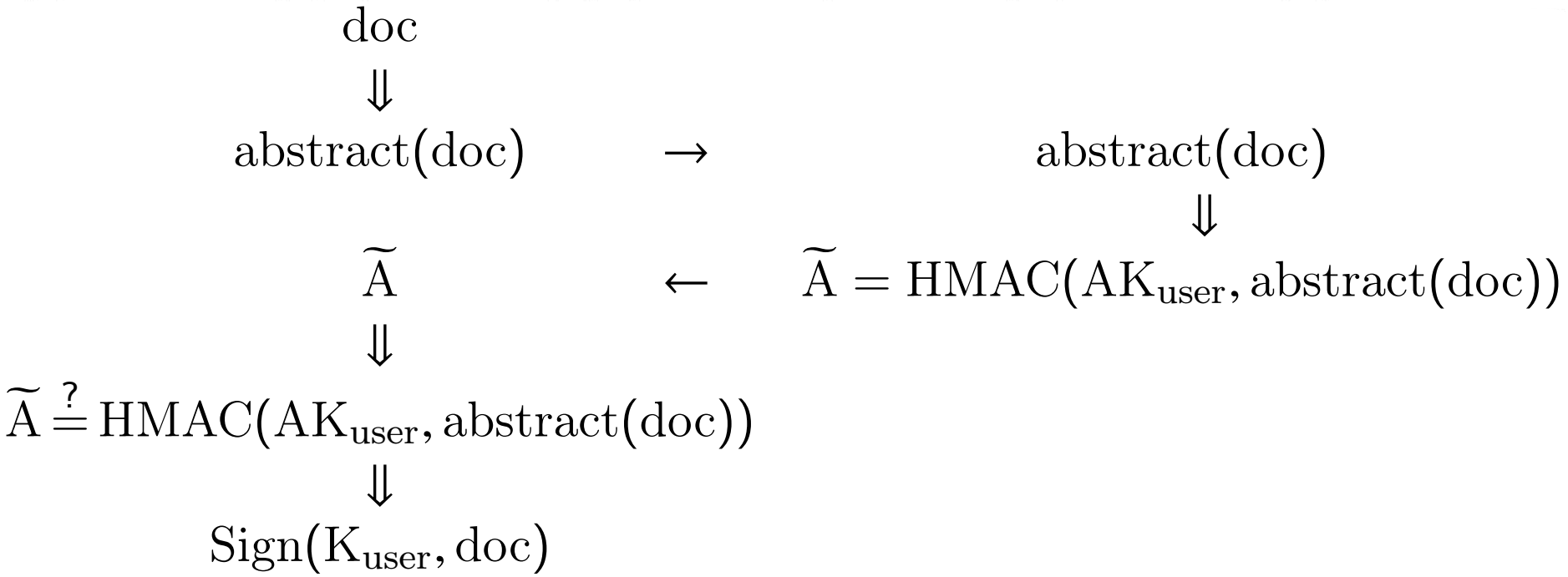
Общий сценарий работы

$$
\begin{array}{ccc}
\text{doc} & & \\
\Downarrow & & \\
\text{abstract(doc)} & \rightarrow & \text{abstract(doc)} \\
 & & \Downarrow \\
\widetilde{\text{A}} & \leftarrow & \widetilde{\text{A}} = \text{HMAC}(\text{AK}_{\text{user}}, \text{abstract(doc)}) \\
\Downarrow & & \\
\widetilde{\text{A}} \stackrel{?}{=} \text{HMAC}(\text{AK}_{\text{user}}, \text{abstract(doc)}) & & \\
\Downarrow & & \\
\text{Sign}(\text{K}_{\text{user}}, \text{doc}) & &
\end{array}
$$

С помощью мобильного устройства:

- аутентифицировать операцию для abstract(doc) и переслать код аутентификации (HMAC) на сервер.
  По документу doc сервер сам вычисляет выжимку и HMAC, проверяет корректность пришедшего кода аутентификации и подписывает документ.

Общий сценарий работы



С помощью мобильного устройства:

- аутентифицировать операцию для abstract(doc) и переслать код аутентификации (HMAC) на сервер.
  По документу doc сервер сам вычисляет выжимку и HMAC, проверяет корректность пришедшего кода аутентификации и подписывает документ.

Почему HMAC_GOSTR3411_2012_256?

- Обоснования стойкости в наиболее сильной модели нарушителя: с атакой с выбором сообщений и угрозой отличения от случайного отображения.
- Уровень априорной стойкости соответствует 256 битам; с явной зависимостью вероятности успеха от допустимых ресурсов (см. «О криптографических свойствах алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012»).
- Не требуется источник случайности на SIM-карте.
- Существенно меньше проблем с побочкой, чем для алгоритма подписи (см. «ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels», D. Genkin et al.)
- Существенно большая производительность на SIM-карте.
- В случае успешной атаки на сервер ключи аутентификации нарушителю уже будут не нужны.

Организация работы с сессионными ключами

Построение дерева ключей: аналогично ESP

„Техническая спецификация по использованию ГОСТ 28147-89 при шифровании вложений в протоколе IPsec ESP“, раздел 5.6. Преобразование ESP_GOST-4M-IMIT.

$$\begin{aligned}
&\text{RootKey}\\
&\text{Divers(}\ \text{RootKey}\ \text{,i\&Mask1)}\\
&\text{Divers(}\ \text{Divers(}\ \text{RootKey}\ \text{,i\&Mask1)}\ \text{,i\&Mask2)}\\
\text{Key[i]} = \text{Divers(}\ &\text{Divers(}\ \text{Divers(}\ \text{RootKey}\ \text{,i\&Mask1)}\ \text{,i\&Mask2)}\ \text{,i\&Mask3)}
\end{aligned}$$

Построение дерева ключей по ТК26АЛГ

KDF_TREE_GOSTR3411_2012_256 в соответствии с Рекомендациями по стандартизации ТК26 «Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012».

Стойкость KDF_TREE_GOSTR3411_2012_256

Модель нарушителя

- Атака: с выбором подмножества известных ключей.
- Угроза: отличение (неизвестного) ключа от случайной строки.
- Ресурсы: 2^{100} в год, 3 года.

В случае дерева на 10^8 ключей

$$\mathrm{Adv}^{\mathrm{PRF}}_{\mathrm{KDF}}(\mathrm{T}, \mathrm{q}, \mathrm{u}) < \frac{2^{106}}{2^{256}} = 2^{-150} \approx 10^{-45}.$$

Стойкость KDF_TREE_GOSTR3411_2012_256

Модель нарушителя

- Атака: с выбором подмножества известных ключей.
- Угроза: отличение (неизвестного) ключа от случайной строки.
- Ресурсы: 2^{100} в год, 3 года.

В случае дерева на 10^8 ключей

$$\mathrm{Adv}^{\mathrm{PRF}}_{\mathrm{KDF}}(\mathrm{T},\mathrm{q},\mathrm{u}) < \frac{2^{106}}{2^{256}} = 2^{-150} \approx 10^{-45}.$$

Трудности с формированием с использованием SIM-карт

Ключ ЭП на SIM-карте: трудности

- Скорость работы эллиптической криптографии на SIM-карте.
- Безопасность реализаций криптографии на эллиптических кривых.
- Качество ДСЧ/ПДСЧ.
- Поддержка разных типов эллиптических кривых, добавление новых кривых.
- Невозможность обеспечения доверенной подписи самого документа — только выжимки (даже если зафиксирован формат, позволяющий однозначно отобразить информативную часть сообщения в выжимку).

Реалистичные опасности при работе с ДСЧ на недоверенной платформе: повторное использование k

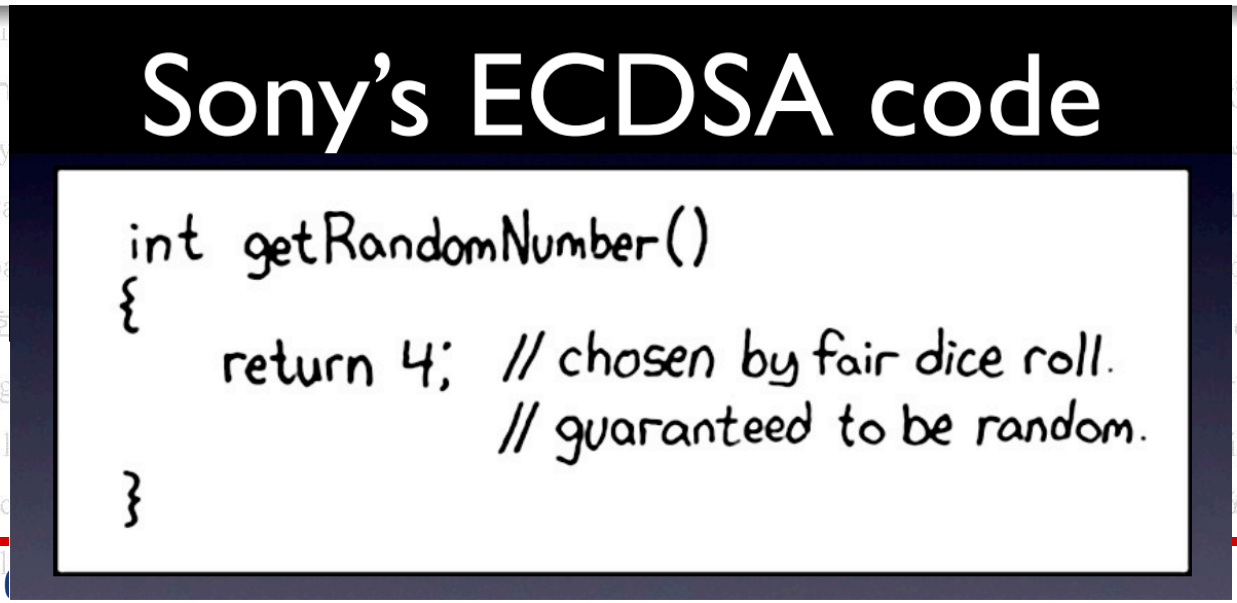
Для сообщений M_1, M_2 с подписями $(r, s_1), (r, s_2)$ из системы

$$\begin{cases} s_1 = rd + k \cdot h(M_1) \bmod q \\ s_2 = rd + k \cdot h(M_2) \bmod q \end{cases}$$

определяются k и d.

2010 год, ошибка в системе подписи кода корпорации Sony

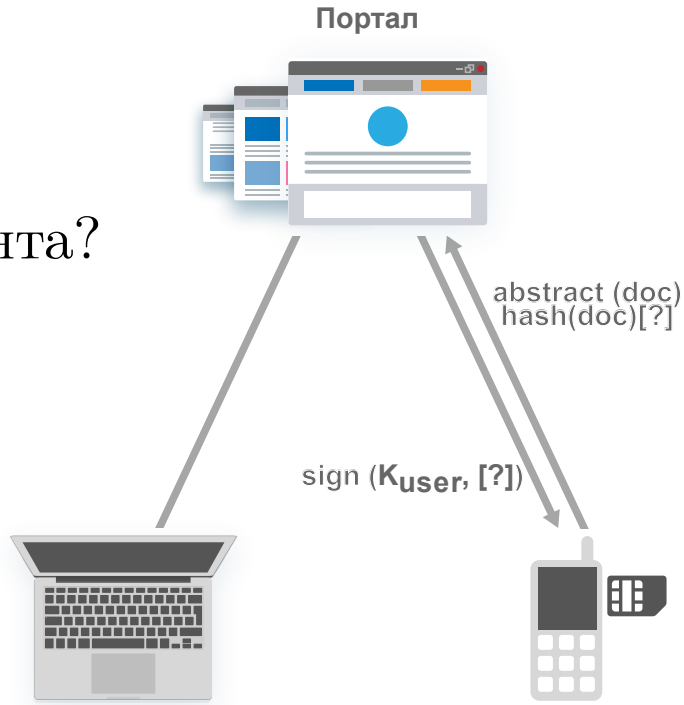
Компрометация ключа подписи дистрибутивов Sony PlayStation 3.



КРИПТО ПРО

Без использования сервера

- Пересылать выжимку и сам документ?
- Пересылать выжимку и хэш от документа?

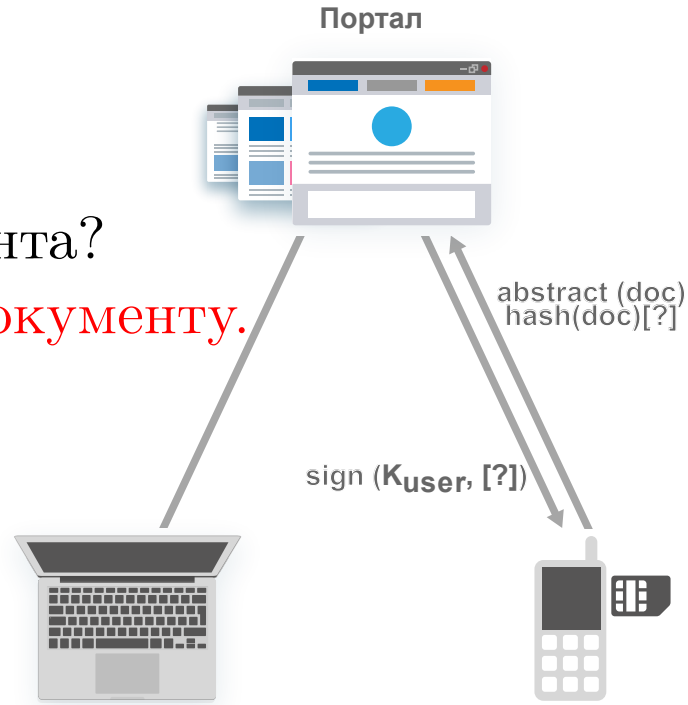


⇒ можно безопасно подтверждать только выжимку, но нельзя подписывать документ (он может быть подменен нарушителем).

КРИПТО ПРО

Без использования сервера

- Пересылать выжимку и сам документ?
  Канал слишком узкий для файла.
- Пересылать выжимку и хэш от документа?
  Не проверить соответствие выжимки документу.



⇒ можно безопасно подтверждать только выжимку, но нельзя подписывать документ (он может быть подменен нарушителем).

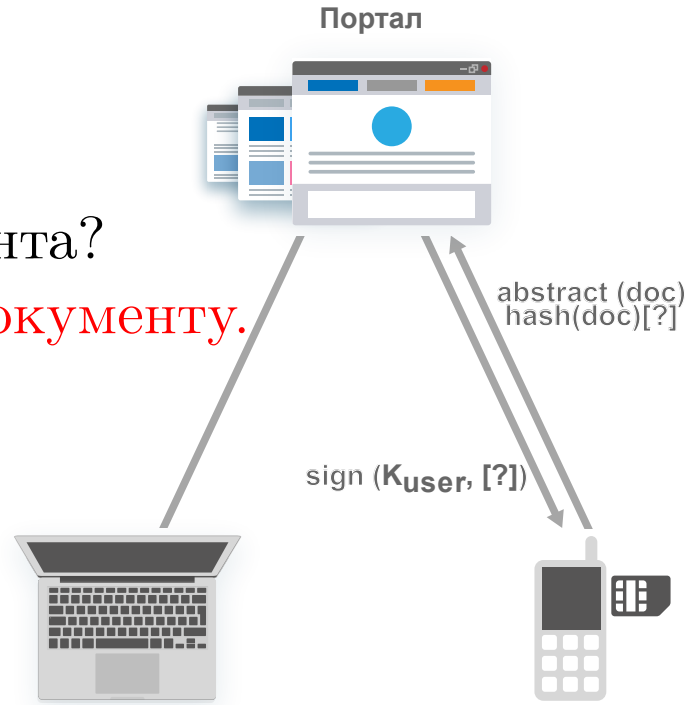
С использованием сервера

Пересылать выжимку от документа, а соответствие выжимки проверять на сервере.

⇒ можно подписывать документ.

Без использования сервера

- Пересылать выжимку и сам документ?
  Канал слишком узкий для файла.
- Пересылать выжимку и хэш от документа?
  Не проверить соответствие выжимки документу.



⇒ можно безопасно подтверждать только выжимку, но нельзя подписывать документ (он может быть подменен нарушителем).

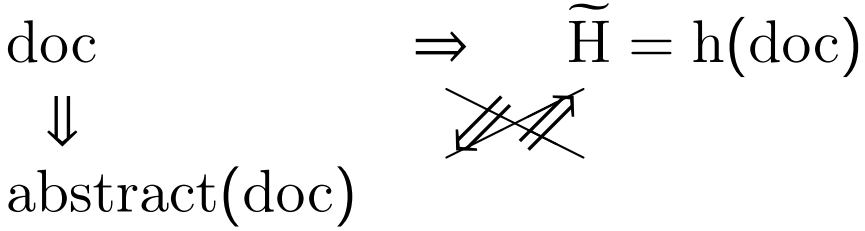
С использованием сервера

Пересылать выжимку от документа, а соответствие выжимки проверять на сервере.

⇒ можно подписывать документ.

КРИПТО ПРО

Без использования сервера

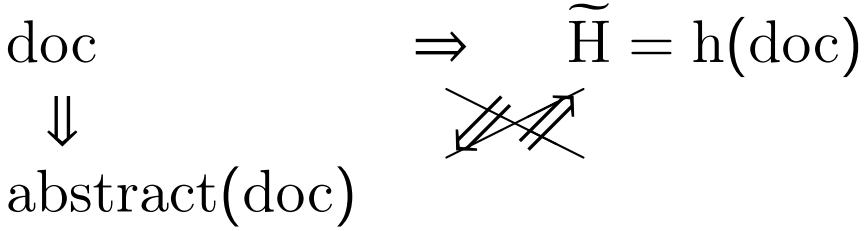


Что подписывать с помощью SIM-карты?

- hash(doc)?
  Не выйдет: сам doc на SIM-карту не попадает.
- $\widetilde{H}$?
  Нет доверия к подписи: соответствие abstract(doc) и $\widetilde{H}$ нельзя установить без doc.
- hash(abstract(doc))?
  Некому подписать сам документ: нет сервера, чтобы, доверившись подписи выжимки, сформировал подпись документа.

КРИПТО ПРО

Без использования сервера



Что подписывать с помощью SIM-карты?

- hash(doc)?
  Не выйдет: сам doc на SIM-карту не попадает.
- $\widetilde{H}$?
  Нет доверия к подписи: соответствие abstract(doc) и $\widetilde{H}$ нельзя установить без doc.
- hash(abstract(doc))?
  Некому подписать сам документ: нет сервера, чтобы, доверившись подписи выжимки, сформировал подпись документа.

КРИПТО ПРО

Без использования сервера

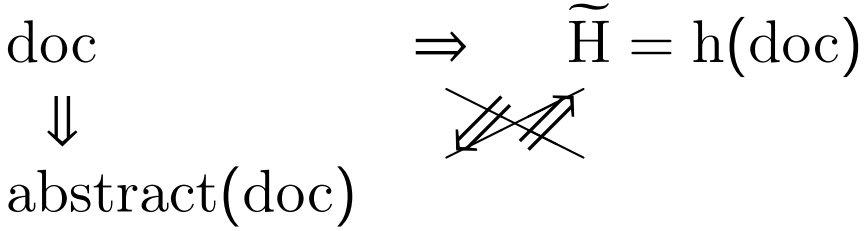
$$\begin{array}{ccc} \text{doc} & \Rightarrow & \widetilde{H} = h(\text{doc}) \\ \Downarrow & \not\Rightarrow & \\ \text{abstract(doc)} & & \end{array}$$

Что подписывать с помощью SIM-карты?

- hash(doc)?
  Не выйдет: сам doc на SIM-карту не попадает.
- $\widetilde{H}$?
  Нет доверия к подписи: соответствие abstract(doc) и $\widetilde{H}$ нельзя установить без doc.
- hash(abstract(doc))?
  Некому подписать сам документ: нет сервера, чтобы, доверившись подписи выжимки, сформировал подпись документа.

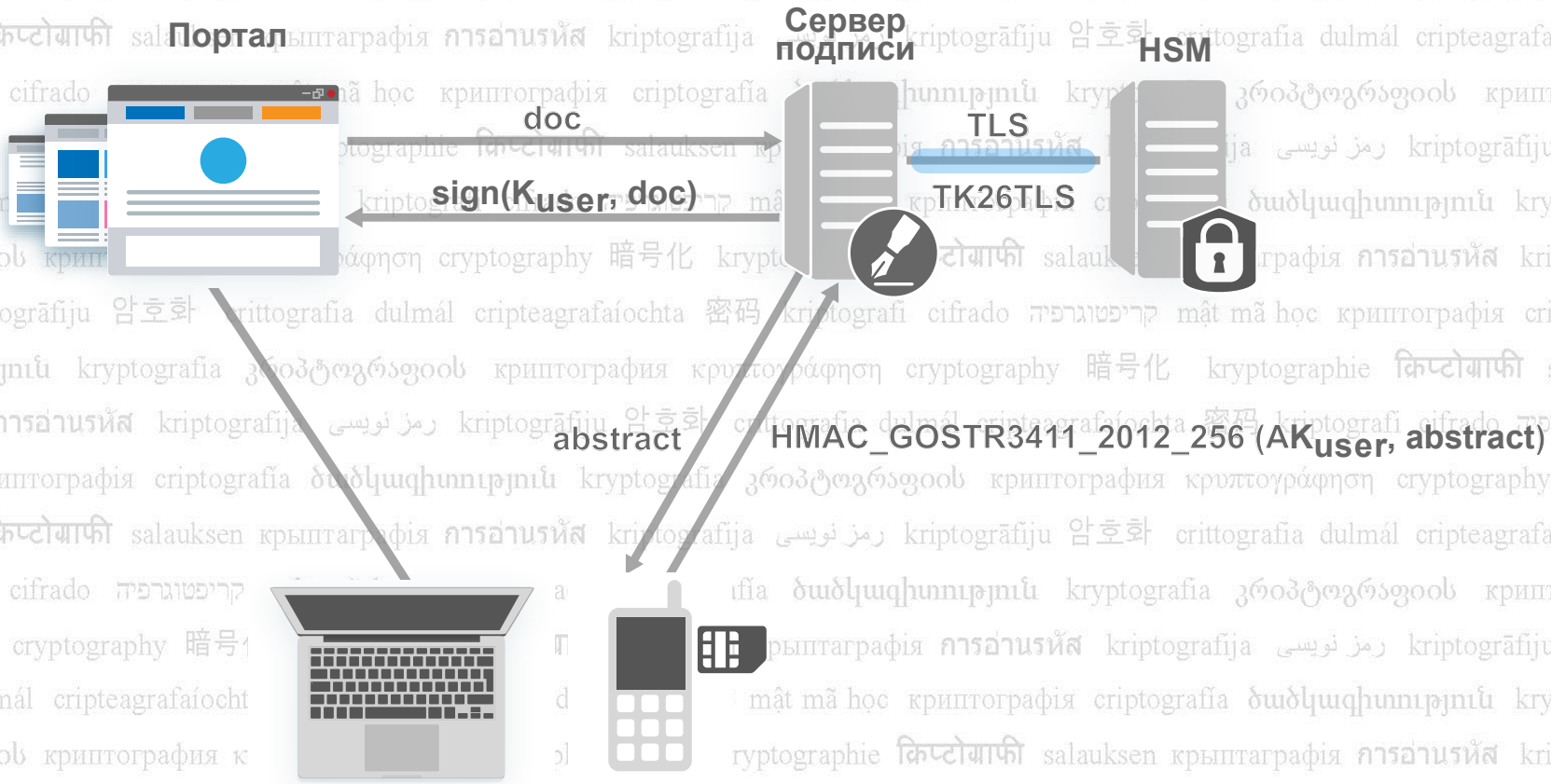
КРИПТО ПРО

Без использования сервера



Что подписывать с помощью SIM-карты?

- hash(doc)?
  Не выйдет: сам doc на SIM-карту не попадает.
- $\widetilde{H}$?
  Нет доверия к подписи: соответствие abstract(doc) и $\widetilde{H}$ нельзя установить без doc.
- hash(abstract(doc))?
  Некому подписать сам документ: нет сервера, чтобы, доверившись подписи выжимки, сформировал подпись документа.



КРИПТО ПРО

С использованием сервера

$$
\begin{array}{ccc}
\text{doc} & & \\
\Downarrow & & \\
\text{abstract(doc)} & \rightarrow & \text{abstract(doc)} \\
 & & \Downarrow \\
\widetilde{\text{A}} & \leftarrow & \widetilde{\text{A}} = \text{HMAC}(\text{AK}_{\text{user}}, \text{abstract(doc)}) \\
\Downarrow & & \\
\widetilde{\text{A}} \stackrel{?}{=} \text{HMAC}(\text{AK}_{\text{user}}, \text{abstract(doc)}) & & \\
\Downarrow & & \\
\text{Sign}(\text{K}_{\text{user}}, \text{doc}) & &
\end{array}
$$

С помощью SIM-карты:

- аутентифицировать операцию для abstract(doc) и переслать код аутентификации (HMAC) на сервер.
  По документу doc сервер сам вычисляет выжимку и HMAC, проверяет корректность пришедшего кода аутентификации и подписывает документ.

С использованием сервера

$$
\begin{array}{ccc}
\text{doc} & & \\
\Downarrow & & \\
\text{abstract(doc)} & \rightarrow & \text{abstract(doc)} \\
 & & \Downarrow \\
\widetilde{\text{A}} & \leftarrow & \widetilde{\text{A}} = \text{HMAC}(\text{AK}_{\text{user}}, \text{abstract(doc)}) \\
\Downarrow & & \\
\widetilde{\text{A}} \stackrel{?}{=} \text{HMAC}(\text{AK}_{\text{user}}, \text{abstract(doc)}) & & \\
\Downarrow & & \\
\text{Sign}(\text{K}_{\text{user}}, \text{doc}) & &
\end{array}
$$

С помощью SIM-карты:

- аутентифицировать операцию для abstract(doc) и переслать код аутентификации (HMAC) на сервер.
  По документу doc сервер сам вычисляет выжимку и HMAC, проверяет корректность пришедшего кода аутентификации и подписывает документ.

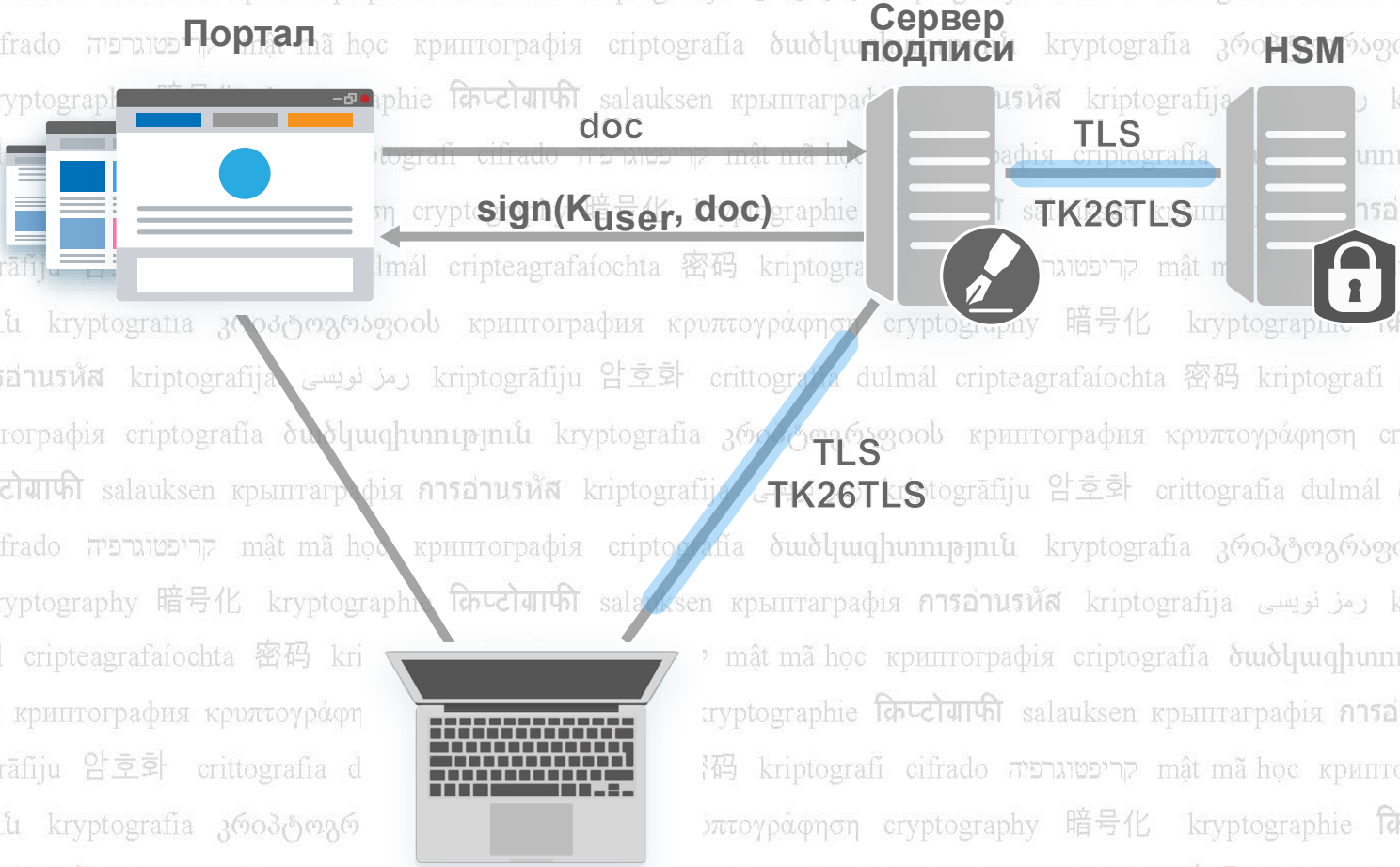
КРИПТО ПРО

Спасибо за внимание!

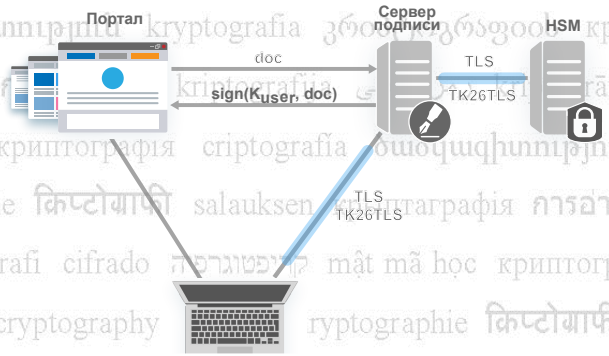
Вопросы?

- Материалы, вопросы, комментарии: svs@cryptopro.ru.

Прямолинейный вариант работы с облаком



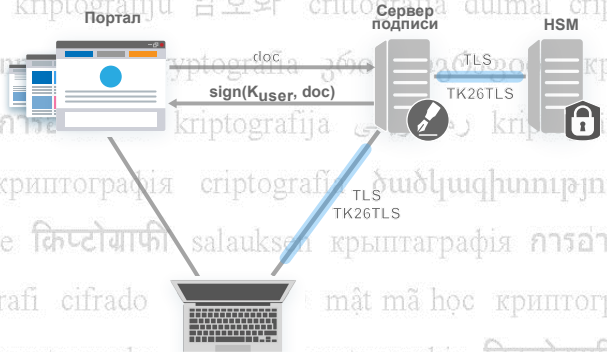
Вопросы доверенной доставки клиентских модулей



Неприменимые решения

- Предположение о существовании защищенного соединения (напр., TLS на основе Рекомендаций ТК 26) не применимо — требует СКЗИ на стороне клиента.
- Общепринятые механизмы на основе хэш-функций защищают только от непреднамеренных искажений.
- Встроенные в ОС системы проверки подписи кода базируются на зарубежной криптографии.

Вопросы доверенной доставки клиентских модулей



Решение

- Предположение: можем один раз доставить самодостаточную утилиту доверенным образом (на физическом носителе).
- Утилита: процедуры проверки подписи, исходный ключ проверки подписи кода.
- На Windows: безопасная интеграция с MS Authenticode, подпись на ГОСТ Р 34.10-2012 в дополнение к подписи на RSA.
- На прочих ОС: отделенная подпись, публикация на сайтах подписей вместо хэшей.
- Процедуры периодической смены ключей

Ремарка: особенности MS Authenticode

Стандартное использование

$$\mathrm{Signature}(\mathrm{Key}, \mathrm{Src}) = \mathrm{Sign}_{\mathrm{RSA-2048}}\left(\mathrm{Key}, \mathrm{h}_{\mathrm{SHA2}}\left(\mathrm{h}_{\mathrm{SHA1}}(\mathrm{Src})|\mathrm{Attrs}\right)\right)$$

Беззатейливое встраивание ГОСТ Р 34.10-2001/2012 по документации MS

$$\mathrm{Signature}(\mathrm{Key}, \mathrm{Src}) = \\ = \mathrm{Sign}_{\text{ГОСТ Р 34.10}}\left(\mathrm{Key}, \mathrm{h}_{\text{ГОСТ Р 34.11}}\left(\mathrm{h}_{\mathrm{SHA1}}(\mathrm{Src})|\mathrm{Attrs}\right)\right)$$

Встраивание ГОСТ Р 34.10-2001/2012 с модификацией штатных механизмов ОС Windows

$$\mathrm{Signature}(\mathrm{Key}, \mathrm{Src}) = \\ = \mathrm{Sign}_{\text{ГОСТ Р 34.10}}\left(\mathrm{Key}, \mathrm{h}_{\text{ГОСТ Р 34.11}}\left(\mathrm{h}_{\text{ГОСТ Р 34.11}}(\mathrm{Src})|\mathrm{Attrs}\right)\right)$$

КРИПТО ПРО

Доверенная визуализация в случае использования SIM-карт

- Узкий канал связи.
- Ограниченность ресурсов по визуализации.
- Пересылка выжимки полей сообщения ⇒ строгая привязка выжимки к сообщению.

Иначе: возможность проведения атак с подменой подписываемых сообщений противоречит принципу персональной ответственности пользователя за подписываемые данные.