Применение протоколов строгой аутентификации на основе неизвлекаемых ключей для разграничения доступа к ресурсам информационных систем

Сергей Панасенко
Компания «Актив»
panasenko@guardant.ru

Компания «Актив»: основные продукты

РУТОКЕН

Идентификаторы и ключевые носители РУТОКЕН: для строгой двухфакторной аутентификации, шифрования и электронной подписи документов (в т.ч. на мобильных устройствах).

30+ миллионов устройств поставлено

Различное программное обеспечение для мониторинга и управления.

guardant

Guardant — ключевое решение для лицензирования и защиты программного обеспечения.

2+

миллионов устройств поставлено

AKTIV. CONSULTING

Консалтинг по информационной безопасности: наши уникальные компетенции и опыт для усиления вашей безопасности.

Разграничение доступа и аутентификация

Разграничение доступа пользователей к ресурсам ИС – одна из основных мер защиты от различного рода деструктивных воздействий:

- информации, обрабатываемой в ИС
- ИС в целом

Пользователи авторизуются на доступ к ресурсам ИС:

- в соответствии с правилами разграничения доступа
- по результатам прохождения идентификации и аутентификации

Требования по разграничению доступа и аутентификации

В соответствии
с Приказом ФСТЭК России
от 25.12.2017 № 239

Обозначения	Меры
I. Идентификация и аутентификация (ИАФ)	
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов
ИАФ.2	Идентификация и аутентификация устройств
ИАФ.3	Управление идентификаторами
ИАФ.4	Управление средствами аутентификации
ИАФ.5	Идентификация и аутентификация внешних пользователей
ИАФ.6	Двусторонняя аутентификация
ИАФ.7	Защита аутентификационной информации при передаче
II. Управление доступом (УПД) (выборка)	
УПД.0	Регламентация правил и процедур управления доступом
УПД.1	Управление учетными записями пользователей
УПД.2	Реализация модели управления доступом
УПД.4	Разделение полномочий (ролей) пользователей
УПД.5	Назначение минимально необходимых прав и привилегий

Проблема: аутентификация на основе уязвимых средств и методов

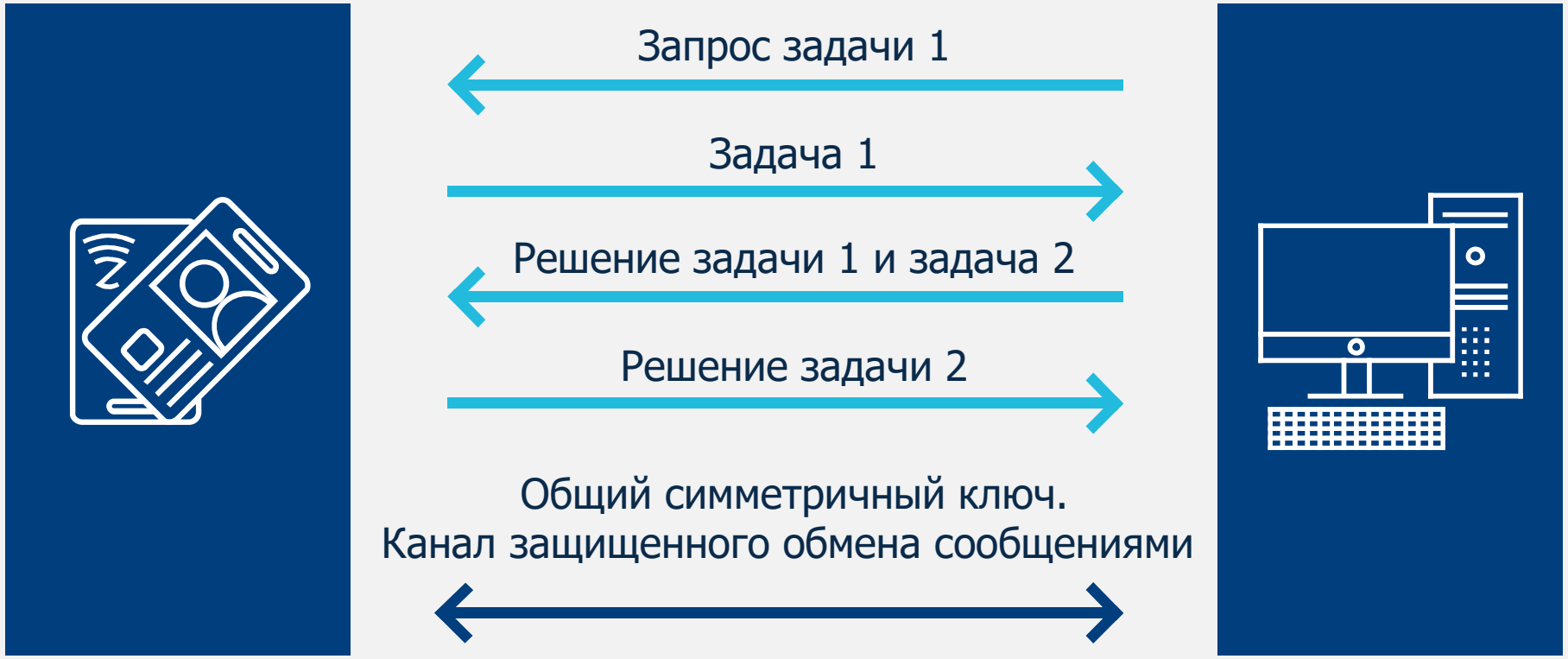
Кража/подделка аутентификационных данных приводит к получению несанкционированного доступа к ресурсам защищаемой системы

Строгая аутентификация

- На основе стандартизованных и доказуемо стойких криптографических протоколов
- С помощью сертифицированных аппаратных средств (смарт-карт, криптографических токенов)
- Носитель защищен от клонирования
- Носитель является активным участником процесса аутентификации
- Возможна взаимная аутентификация
- В результате аутентификации можно получить общий ключ, который впоследствии может быть использован для защиты канала связи
- Ключи не покидают носитель в процессе аутентификации (неизвлекаемые ключи)

В совокупности это позволяет защитить процесс и результаты аутентификации даже от нарушителя очень высокого уровня.

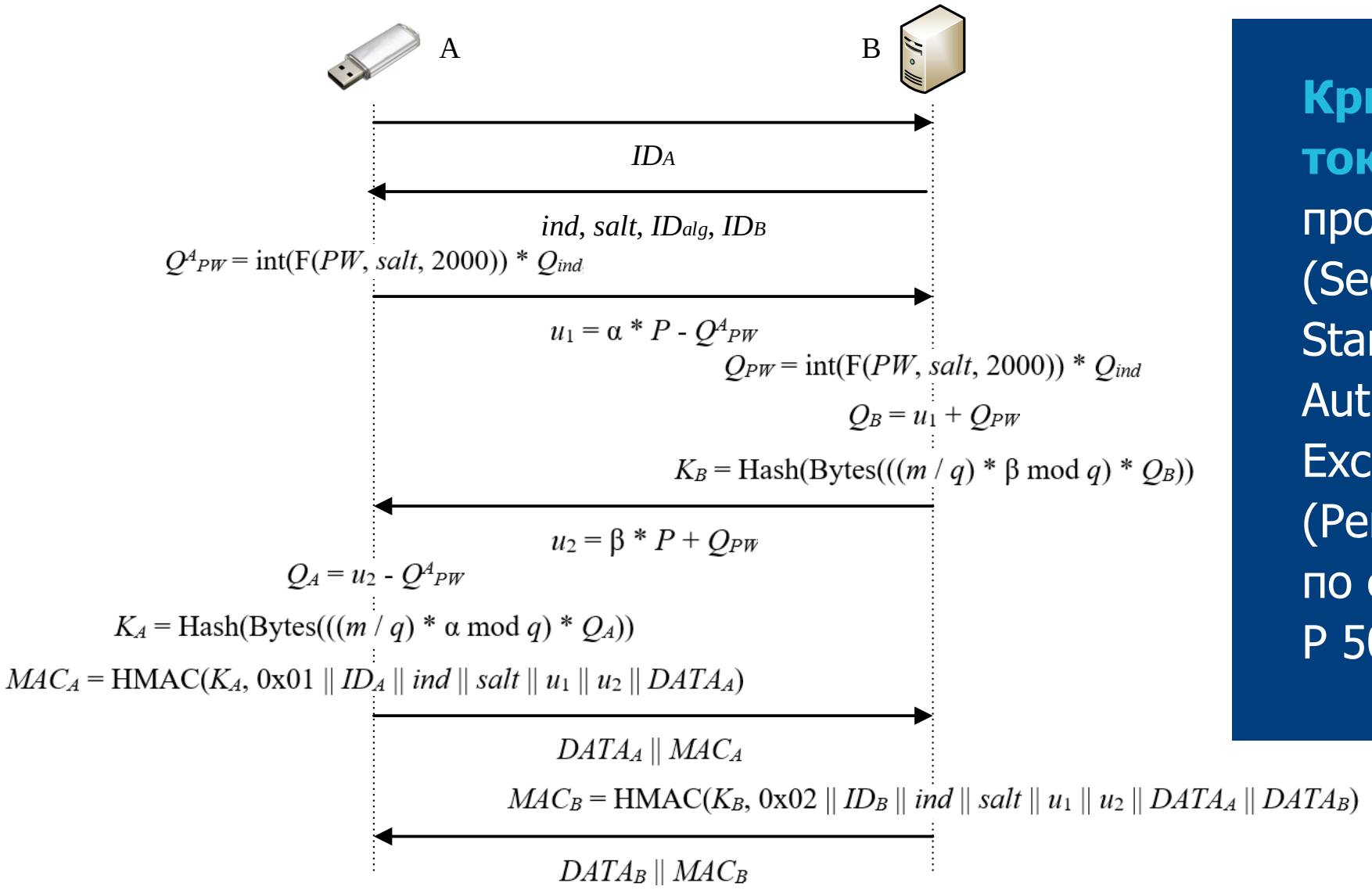
Строгая взаимная аутентификация. Пример 1



Смарт-карты:

режим MUTUAL AUTHENTICATE команд EXTERNAL / GENERAL AUTHENTICATE (ГОСТ Р ИСО/МЭК 7816-4-2013)

Строгая взаимная аутентификация. Пример 2



Криптографический токен:
протокол SESPAKE (Security Evaluated Standardized Password-Authenticated Key Exchange) (Рекомендации по стандартизации Р 50.1.115-2016).

Причины использования уязвимых методов/средств аутентификации

1. Использование устаревших/ унаследованных систем, включая средства защиты.

2. (Кажущаяся) сложность одномоментного перехода на средства, обеспечивающие строгую аутентификацию *.

3. Необходимость вложений в разработку/закупку новых средств защиты, изменения внутренних регламентов, переобучения персонала…

4. Отсутствие должной мотивации на переход на усиленные средства защиты и решение связанных с переходом вопросов.

* Во многих случаях возможен постепенный переход на средства строгой аутентификации в уже развернутых системах.

Криптографические токены/ смарт-карты Рутокен

- Сертифицированные средства аутентификации, многократно апробированные в различных ИС
- Поддержка основных отечественных криптостандартов
- Поддержка стандартизованных протоколов строгой аутентификации
- Защита от клонирования
- Файловая система со средствами разграничения доступа
- Специальные файлы для хранения неизвлекаемых ключей

- Поддержка защищенных каналов обмена сообщениями
- Встроены / поддерживаются в качестве средства аутентификации и носителей ключевой информации в решениях партнеров
- Предоставляется SDK (Software Development Kit) для встраивания
- Консультации / помощь по встраиванию
- Средства мониторинга и управления

Партнерство с разработчиками-лицензиатами ФСТЭК

Разработчик	Продукт
1. Операционные системы	
ГК Астра	Astra Linux
Базальт СПО	ОС Альт
РЕД-СОФТ	РЕД ОС
НТЦ ИТ Роса	Роса
Открытая мобильная платформа	Аврора
2. Виртуальные частные сети	
ИнфоТеКС	VipNet Coordinator, VipNet Client / Client 4u
Код Безопасности	Континент АП, ZTN-клиент
КриптоПро	NGate
Элвис-Плюс	Застава-VPN клиент
С-Терра СиЭсПи	С-Терра Клиент / Клиент А

Разработчик	Продукт
3. Защита каналов связи	
ИнфоТеКС	VipNet PKI Client + VipNet TLS + VipNet УЦ
КриптоПро	NGate VPN Client + NGate + КриптоПро УЦ
4. Защита конечных устройств	
ИнфоТеКС	VipNet SafePoint
Газинформсервис	SafeNode System Loader
5. Комплексная защита физических и виртуальных серверов	
Код Безопасности	VGate

Партнерство с разработчиками-лицензиатами ФСТЭК

Разработчик	Продукт
6. Защита АСУ ТП	
ИнфоТеКС	VipNet SIES
7. Аутентификация пользователей и SSO	
Индид	Indeed Access Manager
Аванпост	Avanpost IDM
8. Управление привилегированными учетными записями	
АйТи Бастион	СКДПУ НТ
Индид	Indeed PAM
9. СУБД	
РЕД-СОФТ	Ред База Данных

Разработчик	Продукт
10. Модули доверенной загрузки и СЗИ от НСД	
Код Безопасности	Соболь, SecretNet Studio, SecretNet LSP
Конфидент	Dallas Lock
ОКБ САПР	Аккорд
Крафтвэй	Витязь
ИнфоТеКС	VipNet SafeBoot
Газинформсервис	Блокхост-Сеть 4
Рубинтех	Страж NT
11. Обеспечение жизненного цикла PKI	
Аванпост	AvanPost PKI
Индид	Indeed CM

Возможности по встраиванию наших продуктов

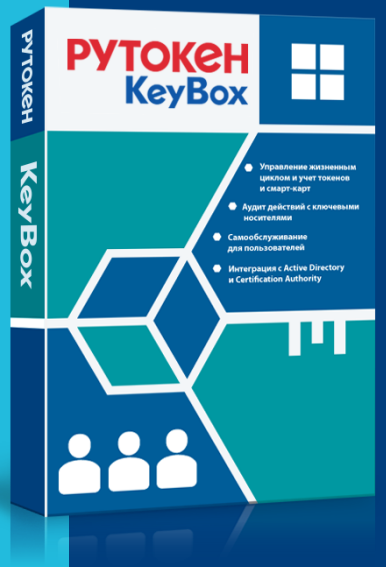
Комплект разработчика Рутокен SDK:

1. Предназначен для встраивания устройств и программного обеспечения Рутокен.
2. Включает набор библиотек (в т. ч. кроссплатформенных) и сервисов, позволяющих производить встраивание на различных уровнях (низкоуровневые, PKCS #11, PC/SC…), утилит для управления устройствами и отладки приложений.
3. Снабжен примерами на различных языках программирования (C/C++/C#, Java, JavaScript).
4. Содержит каркасы для реализации ряда сценариев применения USB-токенов и смарт-карт, бесконтактных NFC- и Bluetooth-устройств в мобильных приложениях, а также каркасы/примеры веб-приложений.
5. Портал документации содержит подробное описание процессов и возможностей встраивания и применения устройств/ПО Рутокен.
6. Демо-портал, позволяет «вживую» посмотреть типичные схемы применения аппаратных решений Рутокен и изучить их основные возможности.
7. Консультирование по встраиванию и применению, техническая поддержка, форум для обсуждения.

Управление средствами аутентификации

Рутокен KeyBox — средство администрирования и управления жизненным циклом ключевых/ аутентифицирующих носителей:

- управление жизненным циклом ключевых носителей — от постановки на учет и ввода в эксплуатацию до вывода из эксплуатации и списания
- управление информацией на ключевых носителях: генерация ключей, запись сертификатов, обновление данных
- управление политиками PIN-кодов носителей
- учет и контроль носителей с ключами и сертификатами, выпущенными сторонними удостоверяющими центрами
- возможность интеграции с внешними системами: СКУД, SSO, IdM/IAM, средствами защиты от НСД, комплексами мониторинга и управления ИБ, кадровыми системами.



Средства защиты информации, использующие аутентифицирующие носители, обычно содержат средства управления ими.

Примеры:

- Avanpost PKI, Avanpost Federated Access Management
- Indeed Certificate Management.

Заключение

1

Одно из необходимых условий обеспечения адекватного уровня безопасности ИС — наличие средств строгой аутентификации пользователей на основе сертифицированных реализаций криптографических протоколов, использующих отечественные криптостандарты и ключи, не извлекаемые из устройств аутентификации.

2

Считаем, что разработчики информационных систем и средств защиты информации должны использовать строгую аутентификацию в своих решениях, а заказчики — требовать наличия средств строгой аутентификации и внедрять их в составе используемых ИС.

Спасибо за внимание!

КОМПАНИЯ АКТИВ

Вопросы?

Сергей Панасенко,

компания «Актив»,
panasenko@guardant.ru