КОМПАНИЯ АКТИВ

Средства аутентификации на примере смарт-карт

Сергей Панасенко
Компания «Актив»
panasenko@guardant.ru

План лекции

1. Аутентификация
2. Смарт-карты
3. Стандарты на смарт-карты
4. Протоколы обмена и форматы данных
5. Криптографические возможности
6. Строгая взаимная аутентификация
7. Защищенный обмен сообщениями
8. Управление криптографическими ключами

Коротко об аутентификации пользователей

Идентификация — это процедура распознавания пользователя по его идентификатору.

Аутентификация — процедура доказательства того, что пользователь на самом деле является тем, за кого он себя выдает.

Виды аутентификации (классификация):

- по этапам: одноэтапная и двухэтапная
- по факторам: однофакторная-двухфакторная-многофакторная
- по сторонам: односторонняя и взаимная
- по методам: простая, усиленная, строгая

Какие могут быть факторы аутентификации:

- нечто, чем мы обладаем (например, уникальный физический объект)
- нечто, что нам известно (например, секретная информация)
- нечто, что является неотъемлемой частью нас самих (биометрия)

Что такое смарт-карты

Смарт-карты — это защищенные микроэлектронные устройства со следующими основными функциями:

- безопасное хранение конфиденциальной информации
- безопасное предоставление конфиденциальной информации различным уполномоченным контрагентам (платежным терминалам, устройствам контроля доступа, валидаторам на транспорте, автоматизированным системам паспортного контроля…)
- выполнение криптографических операций

Смарт-карта — это персональный модуль безопасности ее владельца:

- смарт-карта может вычислять электронную подпись владельца
- смарт-карта может аутентифицировать владельца в различных системах

Обзор стандартов на смарт-карты

Стандарт или семейство стандартов	Название
ГОСТ Р ИСО/МЭК 7810	Карты идентификационные: физические характеристики
ГОСТ Р ИСО/МЭК 7816	1. Семейство основных стандартов для смарт-карт (независимо от применяемого интерфейса): структуры данных, команды, элементы безопасности 2. Физические характеристики, интерфейсы и протоколы для синхронных и асинхронных контактных и USB-карт
ГОСТ Р ИСО/МЭК 10536	Карты поверхностного действия: физические характеристики, интерфейсы и протоколы
ГОСТ Р ИСО/МЭК 14443	Карты ближнего действия: физические характеристики, интерфейсы и протоколы
ГОСТ Р ИСО/МЭК 15693	Карты удаленного действия: физические характеристики, интерфейсы и протоколы

Логическая структура протоколов обмена

Уровни	Протоколы
Прикладной	В зависимости от приложения
Логический	APDU
Транспортный	T=0, T=1
Физический	В зависимости от физического интерфейса

APDU –

Application Protocol Data Unit (*будет подробно описан далее*)

T=0 –

протокол полудуплексной передачи знаков (*должен поддерживаться смарт-картами по умолчанию*)

T=1 –

протокол полудуплексной передачи блоков

Инициатором обмена данными со смарт-картой является терминал:

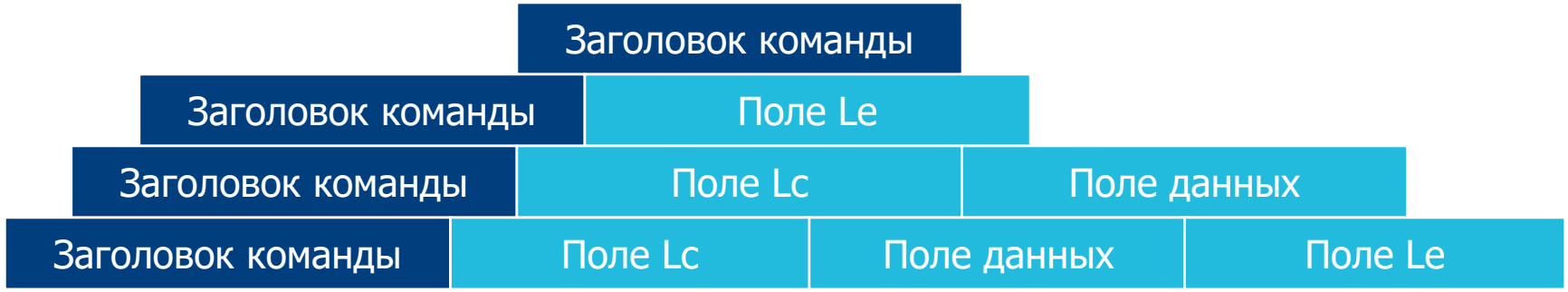
- терминал отправляет на карту APDU-команду
- карта обрабатывает команду и отправляет ответ

Протокол APDU: структура команды

Заголовок команды				Тело команды		
CLA	**INS**	**P1**	**P2**	Lc	Данные	Le

Поле	Размер, байт	Назначение
CLA	1	Класс команды
INS	1	Код команды
P1	1	Параметр команды или код подкоманды/функции
P2	1	Параметр команды/подкоманды/функции
Lc	0/1/3	Размер данных команды (*отсутствует, если данных нет*)
Данные	Lc	Данные команды (*если есть*)
Le	0/1/2/3	Ожидаемый размер данных ответа (*может отсутствовать*)

Протокол APDU: классификация команд



Тип	Lc	Данные команды	Le	Данные ответа
1	–	–	–	–
2	–	–	+	+
3	+	+	–	–
4	+	+	+	+

- Команды могут быть простого и расширенного формата в зависимости от размеров полей Lc и Le.

Протокол APDU: пример команды

APDU-команда SELECT FILE (выбор файла или каталога):

Поле	Значение или назначение
CLA	Значение 00 (hex)
INS	Значение A4 (hex)
P1	Управляет параметрами выбора: ▪ выбор файла по идентификатору ▪ выбор родительского каталога ▪ выбор файла по абсолютному пути ▪ выбор файла по относительному пути
P2	Управление следующими параметрами: ▪ какие данные возвращать в ответе ▪ режим перечисления файлов
Данные команды	Идентификатор/путь к файлу или отсутствует
Данные ответа	В зависимости от значения параметра P2

Протокол APDU: кодировка классов команды

Различные биты в значении класса команды задают следующие режимы:

1 Стандартная или проприетарная команда.

2 Управление сцеплением команд:

- команда является последней или единственной командой в цепочке команд
- команда — не последняя в цепочке команд.

3 Управление защищенным обменом сообщениями (SM — Secure Messaging):

- включение режима SM
- задание подрежимов его работы.

4 Номер логического канала (*карта может поддерживать до 19 логических каналов обмена данными*).

Протокол APDU: структура ответа

Тело ответа	Статус ответа	
Данные	SW1	SW2

Данные в ответе передаются в зависимости от типа команды.
В байтах статуса ответа SW1 и SW2 кодируется результат выполнения команды:

- команда выполнена успешно
- карта готова передать дополнительные данные
- команда выполнена с предупреждением
- возникла ошибка выполнения команды

Пример ответа (на команду записи WRITE BINARY):

Поле	Значение	Описание
Данные	Отсутствуют	
SW1	63 (hex)	Предупреждение: возникла внутренняя ошибка записи
SW2	C3 (hex)	Данные удалось записать после трех повторов записи

TLV — основной формат представления данных

Поле	Размер, байт		Назначение
	Simple TLV	BER-TLV	
Tag	1	1-3	Определяет тип объекта данных
Length	1-3	1-5	Определяет размер объекта данных (*N*)
Value	*N*	*N*	Значение объекта данных (поле отсутствует при *N* = 0)

Основные преимущества TLV:

- компактность
- теги могут быть как глобальными, так и контекстно-зависимыми
- простой формат: легко обрабатывается и конвертируется (*например, в XML*)
- объекты могут быть размещены в любом порядке (*но есть исключения*)
- объекты данных могут быть вложенными

Пример кодирования вложенных структур

Пример кодировки ссылки на объект (для команд работы с объектами, например, COMPARE DATA) (hex): 63 09 92 00 5C 01 80 51 02 12 34

Это набор из четырех вложенных TLV-структур:

Первый уровень вложенности					**Описание**
Tag	Length	Value — второй уровень вложенности			
		Tag	Length	Value	
63	09				Оболочка (wrapper) для составного объекта
		92	00		Локальная ссылка на объект
		5C	01	80	Объект с идентификатором 80
		51	02	1234	Объект в файле с ID 1234

Результат: ссылка на объект 80 в файле 1234 в текущем DF.

Категории стандартных APDU-команд

1. Выбор объекта данных или логического канала.
2. Операции с бинарными файлами.
3. Операции с файлами записей.
4. Операции с объектами данных.
5. Основные и расширенные команды обеспечения безопасности.
6. Управление передачей данных.
7. Управление жизненным циклом карты и файлов.
8. Управление приложениями.
9. Операции с базами данных.

Основные команды обеспечения безопасности: команды аутентификации

Команда	Назначение
INTERNAL AUTHENTICATE	Аутентификация карты терминалом
GET CHALLENGE	Запрос задачи для последующей аутентификации терминала или взаимной аутентификации
EXTERNAL AUTHENTICATE	Аутентификация терминала картой (на основе выданной ранее задачи)
GENERAL AUTHENTICATE	Аутентификация карты терминалом, аутентификация терминала картой или взаимная аутентификация
VERIFY	Аутентификация путем сравнения внешних данных (например, пароля или отпечатка пальца) с данными, хранящимися в карте

Основные команды обеспечения безопасности: прочие команды

Команда	Назначение
CHANGE REFERENCE DATA	Обновление хранящихся в карте данных, относящихся к обеспечению безопасности
ENABLE/DISABLE VERIFICATION REQUIREMENT	Включение/отключение требования о необходимости сравнения данных
RESET RETRY COUNTER	Сброс счетчика попыток предъявления внешних данных
MANAGE SECURITY ENVIRONMENT	Настройка компонентов, сохранение/восстановление или удаление среды безопасности

Расширенные команды обеспечения безопасности

Команда	Назначение
GENERATE ASYMMETRIC KEY PAIR	Генерация пары асимметричных ключей или запрос открытого ключа сгенерированной ранее пары
PERFORM SECURITY OPERATION (PSO)	Вычисление или проверка криптографической контрольной суммы, электронной подписи или хеш-кода, зашифрование или расшифрование

Операции команды PSO

Операция	Назначение
COMPUTE CRYPTOGRAPHIC CHECKSUM	Вычисление криптографической контрольной суммы
COMPUTE DIGITAL SIGNATURE	Вычисление электронной подписи (в т.ч. в комбинации с предварительным хешированием)
HASH	Хеширование
VERIFY CRYPTOGRAPHIC CHECKSUM	Проверка криптографической контрольной суммы
VERIFY DIGITAL SIGNATURE	Проверка электронной подписи (в т.ч. в комбинации с предварительным хешированием)
VERIFY CERTIFICATE	Проверка сертификата открытого ключа
ENCIPHER	Зашифрование
DECIPHER	Расшифрование

Команды управления передачей данных

Команда	Назначение
GET RESPONSE	Запрос APDU-ответа на ранее выполненную команду или его части
ENVELOPE	Передача вложенной команды или объекта

Передача вложенной команды

Строгая взаимная аутентификация

Режим MUTUAL AUTHENTICATE команд:

- EXTERNAL AUTHENTICATE
- GENERAL AUTHENTICATE

Защищенный обмен сообщениями

Задачи, решаемые защищенным обменом сообщениями (Secure Messaging, SM):

1. Контроль целостности / аутентификация данных с помощью криптографических контрольных сумм (Cryptographic Checksum, CCS).
2. Защита целостности и конфиденциальности данных с помощью криптограмм.

В структуру APDU-запросов/ответов добавляются CCS и криптограммы (*будет описано далее*).

Варианты защиты APDU-ответа:

1. Без обеспечения целостности APDU-ответа.
2. С обеспечением целостности APDU-ответа.

Признак использования SM указывается в классе APDU-команды.

Обозначения:

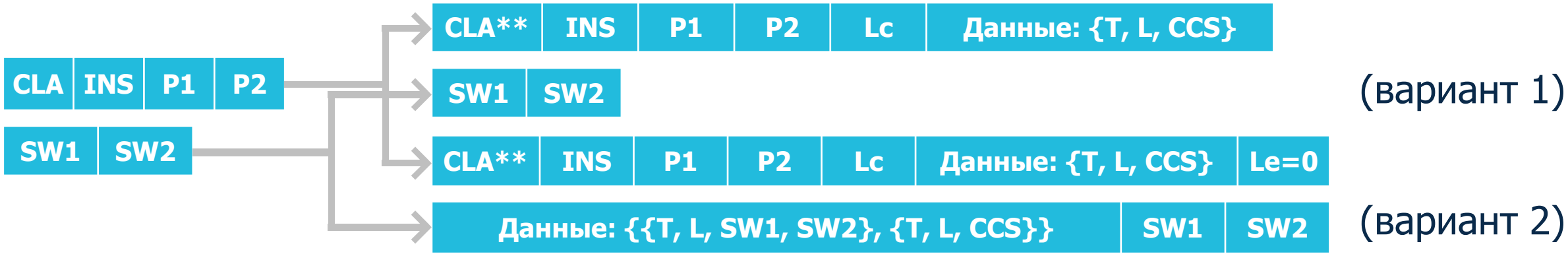
CLA – класс исходной команды

CLA* – используется SM, заголовок APDU-команды не включается в расчет CCS

CLA** – используется SM, заголовок APDU-команды включается в расчет CCS

Аутентификация данных с помощью SM

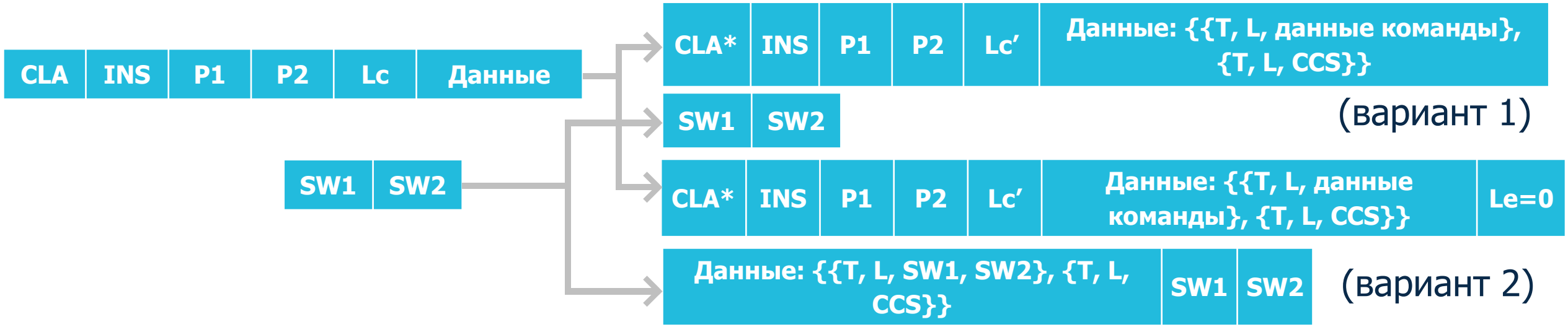
Команда типа 1 (данных нет):



Команда типа 2 (нет данных команды, есть данные в ответе):

Аутентификация данных с помощью SM

Команда типа 3 (есть данные в команде, нет данных ответа):



Команда типа 4 (есть данные и в команде, и в ответе):

Шифрование данных с помощью SM

Команда типа 2 (нет данных команды, есть данные в ответе):

Команда типа 3 (есть данные в команде, нет данных ответа):

Команда типа 4 (есть данные и в команде, и в ответе):

- Может быть обеспечена конфиденциальность заголовка APDU-команды путем ее помещения в виде зашифрованных данных в команду ENVELOPE.

Варианты получения ключей

Ключи могут быть:

1 **Загружены на смарт-карту заранее, в т. ч. с помощью следующих команд:**

- CHANGE REFERENCE DATA (позволяет записать на карту симметричный ключ)
- PUT DATA (позволяет записать на карту секретный асимметричный ключ)

2 **Сгенерированы смарт-картой:** команда GENERATE ASYMMETRIC KEY PAIR позволяет сгенерировать пару асимметричных ключей непосредственно картой *(секретный ключ такой пары может быть неизвлекаемым)*

3 Получены смарт-картой и компьютером в рамках выполнения процедуры взаимной аутентификации (команда GET CHALLENGE + режим MUTUAL AUTHENTICATE и другие варианты)

4 **Получены динамически иными способами, например:**

- генерацией секретного ключа с помощью ДСЧ карты и его считывание командой GET DATA
- явным применением протоколов обмена ключами, например, ECDH/ECKEP
- диверсификацией ключей…

Заключение

1. Аутентификация пользователя – процедура подтверждения идентификации пользователя (доказательства, что пользователь является тем, за кого он себя выдает).

2. Смарт-карты – это защищенные микроэлектронные устройства, обычно снабжены набором функций по обеспечению безопасности. Могут быть использованы для строгой аутентификации пользователей.

3. Для взаимодействия со смарт-картами на логическом уровне используются APDU-команды.

4. Смарт-карты могут поддерживать широкий спектр криптографических операций, включая реализации алгоритмов и протоколов аутентификации, шифрования, хеширования и электронной подписи, а также поддержку защищенного обмена сообщениями.

Спасибо за внимание!

КОМПАНИЯ АКТИВ

Вопросы?

Сергей Панасенко

Компания «Актив»

panasenko@guardant.ru

КОМПАНИЯ АКТИВ

Компания «Актив» — крупнейший в России производитель аппаратных средств электронной подписи и решений для защиты программного обеспечения. Компания на рынке уже 30 лет.

Сейчас в компании работает более 250 человек.
Из них около трети — разработчики, тестировщики и технические аналитики.

Средний возраст IT специалистов в компании — менее 30 лет.
Компания активно нанимает в том числе студентов старших курсов.
Многие руководители и лиды групп приходили работать в «Актив» студентами на позиции младших разработчиков, тестировщиков.

Компания «Актив» славится своим коллективом: здесь всегда готовы помочь разобраться в трудной проблеме, дать совет, подставить плечо.
Каждый участник команды имеет право голоса, будет выслушан и может влиять на процессы. Именно за счёт новых идей, участия молодых сотрудников компания идёт в ногу со временем и применяет современные методы и технологии в процессах разработки.

Если у Вас возник интерес к нашей компании, и Вы хотите стать ее частью, проходите по ссылке в QR-коде и присылайте резюме!