ПЛАН РАБОТЫ РАБОЧЕЙ ГРУППЫ ПО СТАНДАРТИЗАЦИИ ПРИМЕНЕНИЯ РОССИЙСКИХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ В НАЦИОНАЛЬНОЙ СИСТЕМЕ ПЛАТЕЖНЫХ КАРТ (НСПК)

Тема/Задача: Разработка аналога стандарта EMV, а также других стандартов необходимых для устойчивого функционирования национальной системы платежных карт

Разработка аналога стандарта EMV, а также других карточных стандартов необходимых для устойчивого функционирования национальной системы платежных карт, должна включать следующий комплекс взаимосвязанных работ (мероприятий), обеспечивающих получение необходимых результатов.

Отработка отдельных мероприятий без проработки иных не позволяет получить требуемые промышленные решения.

	Наименование мероприятия	Основной результат выполнения мероприятия	Примечание
1	Перевод и научно-техническое редактирование следующих эталонных спецификаций (*наименования и состав может быть уточнен в ходе проведения работ*): - GlobalPlatform (SCP, токены); - Common Payment Application; - Common Personalization Specification; - 3 D Secure; - Chip Authentication Program/Dynamic Passcode Authentication; - генерация криптотокенов карты – MACing сообщений, генерация/верификация CVN, PVV и шифрование ПИН-кодов; - Format Preserving Encryption.	Переводы текстов эталонных спецификаций (*общим объемом ориентировочно до 500 листов текста документов*) с разметкой примитивов безопасности (полей заголовков и/или типовых протокольных блоков данных - APDU), формируемых и/или обрабатываемых с применением криптографических алгоритмов, определенных соответствующими международными стандартами (ISO/IEC 9796, ISO/IEC 9797, ISO/IEC 10116, ISO/IEC 10118 и др.)	
2	Разработка инструментов криптоанализа: - Общее описание ключевой сети	Описание ключевой сети системы платёжных карт.	

	Наименование мероприятия	Основной результат выполнения мероприятия	Примечание
	системы платёжных карт, - Разработка частных моделей нарушителя элементов национальной системы платёжных карт	Частные модели (по платёжной карте, терминалам, различным участкам работы с платёжными картами и платёжными транзакциями в АБС)	
3	Разработка предложений по вариантам формирования протокольных примитивов безопасности (полей заголовков и/или типовых протокольных блоков данных - APDU), формируемых и/или обрабатываемых с применением криптографических алгоритмов, на основе аналогичных российских спецификаций криптографических алгоритмов и протоколов безопасности, базирующихся на данных алгоритмах (требований документов ГОСТ Р и/или методических рекомендаций ТК 26 «Криптографическая защита информации»).	Переработанные русскоязычные тексты эталонных спецификаций, включающие положения (с заменой и/или дополнением существующих требований), которые определяют порядок формирования и/или обработки примитивов безопасности (полей заголовков и типовых протокольных блоков данных - APDU) с использованием криптографических алгоритмов, на основе российских спецификаций (ГОСТ Р) криптографических алгоритмов и протоколов безопасности, базирующихся на данных алгоритмах	
3.1	Разработка рекомендаций 1) выработки секретных и открытых ключей подписи эмитентов, эквайреров, карт, УЦ, 2) формирования ключевых контейнеров секретных ключей, 3) формирования и проверки сертификатов ОК, 4) выработки мастер-ключей карты из мастер-ключей эмитентов, 5) формирования и подписи данных статической аутентификации карты (SDA), 6) формирования мастер-ключей карты для персонализации карт, 7) формирования сессионных ключей для	Согласованные рекомендации и форматы по применению криптоалгоритмов на участках предперсонализации и персонализации чиповых карт в АБС	

	Наименование мероприятия	Основной результат выполнения мероприятия	Примечание
	персонализации карты, 8) шифрования секретных данных и APDU, а также алгоритмы имитозащиты при персонализации, 9) генерации криптотокенов карты.		
3.2			
	Разработка рекомендаций 1) формирования сессионных ключей карты из мастер-ключей карты, 2) формирования и проверки прикладных криптограмм, 3) шифрования и имитозащиты секретных сообщений (в том числе для Script Processing), 4) шифрования и верификации PIN при on-line и off-line проверке PIN, 5) верификации DAC при статической аутентификации, 6) верификации DN, 7) шифрования и имитозащиты PIN при передаче между PED и ридером.	Согласованные рекомендации и форматы по применению криптоалгоритмов при проведении процессинга по чип-картам	
3.3			
	Разработка рекомендаций 1) формирования CVV/CVC, 2) шифрования и проверки PIN, 3) формирования и проверки PVV, 4) выработки мастер ключа карты MK-CVC3 из мастер-ключа эмитента , 5) генерации IVCVC3 (Initial Vector Card Verification Code) и статического CVC3, 6) генерации IVCVC3 (Initial Vector Card Verification Code) и динамического dCVC3, 7) выработки симметричных ключей и	Согласованные рекомендации и форматы по применению криптоалгоритмов при эмиссии и процессинге карт с магнитной полосой и бесконтактных карт	

	Наименование мероприятия	Основной результат выполнения мероприятия	Примечание
	аутентификации терминалов/банкоматов 8) имитозащиты сообщений транзакции		
3.4			
	Разработка рекомендаций 1) формирования и имитозащиты сообщений при проведении операции по протоколу 3-D Secure (аналог MAC/HMAC для сообщений AAV/CAVV) 2) выработки одноразовых паролей (технологии CAP/DPA)	Согласованные рекомендации и форматы по применению криптоалгоритмов при поддержке технологии 3-D Secure	
3.5			
	Разработка рекомендаций 1) формирования проверочных величин ключей 2) шифрования PIN для хранения в БД 3) формирования проверочной величины PIN 4) формирования ключа из пароля 5) экспорта/импорта ключей - на симметричном ключе; - на ключе из пароля 6) экспорта/импорта PIN-блоков: - на симметричном ключе; - на ключе из пароля	Согласованные рекомендации и форматы по вспомогательным криптопрцедурам	
4.	Тестирование производительности российских криптопримитивов, используемых взамен зарубежных, для наиболее критичных элементов системы платёжных карт	Таблица сравнительных результатов производительности	Требуется участие производителей чип-карт
	Подготовка предложений по корректировке требований Банка России в части замены технологий, рекомендуемых для использования в банках, присоединяющихся к НСПК	Согласованные предложения	

	Наименование мероприятия	Основной результат выполнения мероприятия	Примечание
	Подготовка предложений по сертификации алгоритмов и оборудования в части соответствия требованиям EMVCo и NIST	Согласованные предложения	Для внесения в нормативные документы Банка России, регулирующего платёжный процесс
7	Подготовка обращения с просьбой о создании стенда апробации новых платёжных технологий	Подготовленные предложения	