

УТВЕРЖДАЮ

Генеральный директор
ООО "Криптоком"



2014 г.

Д.Б. Кабелев

УТВЕРЖДАЮ

Генеральный директор
ООО "КРИПТО-ПРО"



" " 2014 г.

Н.Г. Чернова

ПРОТОКОЛ

испытаний соответствия реализации CMS и X.509 методическим
рекомендациям ТК26 и обеспечения встречной работы

Москва, 2014

Общество с ограниченной ответственностью "Криптоком" (ООО "Криптоком") и общество с ограниченной ответственностью "КРИПТО-ПРО" (ООО "КРИПТО-ПРО") провели совместные испытания СКЗИ "МагПроКриптоПакет 3.0" и СКЗИ "КриптоПро CSP 4.0" на соответствие требованиям методических рекомендаций ТК26 по использованию российских криптографических алгоритмов при работе с форматами CMS, X.509.

Участники испытаний:

- от ООО "Криптоком":

Устинов Игорь Геннадьевич, заместитель генерального директора;

- от ООО "КРИПТО-ПРО":

Смышляев Станислав Витальевич, начальник отдела защиты информации.

1. Проведены испытания СКЗИ "МагПроКриптоПакет 3.0" (программное обеспечение, установленное на ОС семейства Linux) и СКЗИ "КриптоПро CSP4.0" (программное обеспечение, установленное на ОС семейства WindowsNT) на основании документов:

- [CMS] Методические рекомендации. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS;

- [X.509] Техническая спецификация использования алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509;

- [ALG] Методические рекомендации по криптографическим алгоритмам, сопутствующим применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012.

2. Во время испытаний проверены пункты рекомендаций, включая все обязательные пункты, со следующими результатами.

Каждый участник испытаний осуществлял формирование сообщений для другого участника и проверку сообщений, полученных от другого участника, по всем пунктам таблицы.

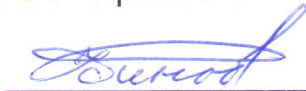
	Пункт рекомендаций	Содержание проверяемого пункта рекомендаций	Результаты
1	Алгоритмы хэширования сообщений		
1.1	4.1 [CMS]	Хэширование сообщений на основе алгоритма ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит	Проверено

1.2	4.2 [CMS]	Хэширование сообщений на основе алгоритма ГОСТ Р 34.11-2012 с длиной хэш-кода 512 бит	Проверено
2	Формирование и проверка сертификатов субъекта		
2.1	4.3 [X.509]	Формирование и использование сертификатов ключей с идентификатором id-tc26-gost3410-2012-256	Проверено
2.2	4.3 [X.509]	Формирование и использование ключей с идентификатором id-tc26-gost3410-2012-512	Проверено
3	Алгоритмы управления ключами и шифрования содержимого		
3.1	4.3 [X.509] 5.3.1 [ALG] 6.2 [CMS] 7.1 [CMS]	Передача и прием защищенного сообщения при использовании алгоритма передачи ключей на основе VKO_GOSTR3410_2012_256 для открытых ключей с идентификатором id-tc26-gost3410-2012-256	Проверено
3.2	4.3 [X.509] 5.3.1 [ALG] 6.2 [CMS] 7.1 [CMS]	Передача и прием защищенного сообщения при использовании алгоритма передачи ключей на основе VKO_GOSTR3410_2012_256 для открытых ключей с идентификатором id-tc26-gost3410-2012-512	Проверено
4	Алгоритмы формирования и проверки подписи		
4.1	4.3 [X.509] 5.1 [CMS]	Формирование и проверка подписанного сообщения с использованием ГОСТ Р 34.10-2012 с ключом 256 бит (для открытых ключей с идентификатором id-tc26-gost3410-2012-256)	Проверено
4.2	4.3 [X.509] 5.2 [CMS]	Формирование и проверка подписанного сообщения с использованием ГОСТ Р 34.10-2012 с ключом 512 бит (для открытых ключей с идентификатором id-tc26-gost3410-2012-512)	Проверено

3. Общий вывод участников испытаний: СКЗИ "МагПро КриптоПакет 3.0" и СКЗИ "КриптоПро CSP" соответствуют требованиям рекомендаций ТК26 по реализации протоколов CMS и X.509 и обеспечивают возможность встречной работы.

Подписи участников испытаний:

- от ООО "Криптоком":

 Устинов Игорь Геннадьевич,
заместитель генерального директора

- от ООО "КРИПТО-ПРО":

 Смышляев Станислав Витальевич,
начальник отдела защиты информации