

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ)
«РУТОКЕН ЭЦП»

ФОРМУЛЯР

КБДЖ.468244.044 ФО

Изделие: «Средство криптографической защиты информации «РУТОКЕН ЭЦП»

Формуляр: КБДЖ.468244.044 ФО

© ЗАО «Актив-софт»

Вторая редакция: апрель 2011

Фирма оставляет за собой право вносить изменения в содержание данного документа без уведомления потребителей.

1. Общие сведения

1.1. ОБЩИЕ СВЕДЕНИЯ ПО ИЗДЕЛИЮ.

Наименование изделия: «Средство криптографической защиты информации (СКЗИ) «РУТОКЕН ЭЦП».

Обозначение: КБДЖ.468244.044.

Наименование предприятия разработчика и изготовителя:
ЗАО «Актив-софт».

Заводской номер: см. Приложение №1.

Регистрационный номер: 3883- 030150
3883- 030649

Дата изготовления: _____

1.2. ТРЕБОВАНИЯ К ВЕДЕНИЮ ФОРМУЛЯРА И МЕСТУ ЕГО ХРАНЕНИЯ.

Формуляр должен находиться в подразделении, ответственном за эксплуатацию изделия. Все записи в формуляре производятся от руки разборчиво и аккуратно. Подписки и заверенные исправления не допускаются. Неправильная запись должна быть аккуратно зачеркнута и рядом записана новая, которую заверяет ответственное лицо. После подписи представляются фамилию и инициалы ответственного лица (вместо подписи допускается проставлять личный штамп исполнителя).

1.3. ПЕРЕЧЕНЬ ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ, С КОТОРОЙ ДОЛЖЕН БЫТЬ ОЗНАКОМЛЕН ПЕРСОНАЛ.

Перед эксплуатацией изделия необходимо ознакомиться с документами:

- СКЗИ «РУТОКЕН ЭЦП». Правила пользования. КБДЖ.468244.044.
- Автоматизированное рабочее место загрузки ключевой информации (АРМ ЗКИ) в аппаратный модуль (АМ) «РУТОКЕН ЭЦП». Правила пользования. КБДЖ.468244.046.
- АМ «РУТОКЕН ЭЦП». Инструкция по встраиванию. КБДЖ.00610-0100 33.
- Программный модуль АРМ ЗКИ «РУТОКЕН ЭЦП». Руководство администратора. КБДЖ.00610-0100 99.
- Драйвер «РУТОКЕН» для SC API. Руководство пользователя. КБДЖ.00179-0310 34.
- Драйвер шифрования «РУТОКЕН» для Scurtop API. Руководство пользователя. КБДЖ.00182-0110 34.

2. Основные характеристики

2.1. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ИЗДЕЛИЯ.

СКЗИ «РУТОКЕН ЭЦП» подключается по шине USB к ПЭВМ и предназначено для вычисления и проверки электронной цифровой подписи (ЭЦП).

ОГЛАВЛЕНИЕ

1.	Общие сведения	3
2.	Основные характеристики	3
3.	Комплектность	5
4.	Свидетельство о приемке	6
5.	Гарантийные обязательства	7
6.	Отметка о продаже	7

шифрования и безопасного хранения данных. Для обеспечения функций шифрования, ЭЦП и зашифрования в устройстве реализованы алгоритмы ГОСТ 28147-89, ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94.

Изделие СКЗИ «РУТОКЕН ЭЦП» обеспечивает:

- хранение во внутренней памяти информации, передаваемой в изделие через USB порт ПЭВМ;
- шифрование и выработку случайных чисел по стандарту ГОСТ 28147-89;
- вычисление и проверку имитовставки по стандарту ГОСТ 28147-89;
- вычисление и проверку ЭЦП по стандарту ГОСТ Р 34.10-2001;
- вычисление значения хэш-функции по стандарту ГОСТ 34.11-94;
- выработку сессионных ключей (ключей парной связи) по схеме VKO ГОСТ Р 34.10-2001 (RFC 4357);
- выработку ключей шифрования внутри изделия и их защищенное хранение без возможности экспорта.

СКЗИ «РУТОКЕН ЭЦП» предполагается использовать при работе в составе средств автоматического создания и проверки электронной подписи.

В СКЗИ «РУТОКЕН ЭЦП» контроль срока использования ключа электронной подписи, блокирующего работу СКЗИ «РУТОКЕН ЭЦП» в случае попытки использования ключа дольше заданного срока, обеспечивается организационно-техническими мерами.

2.2. КОЛИЧЕСТВЕННЫЕ И КАЧЕСТВЕННЫЕ ХАРАКТЕРИСТИКИ ИЗДЕЛИЯ.

Алгоритм шифрования	ГОСТ 28147-89, режимы простой замены, гаммирования, гаммирования с обратной связью и выработки имитовставки
Скорость криптографического преобразования данных	Не менее 30 Кбайт/сек
Требования к средствам защиты конфиденциальной информации	По классу защиты КС2
Поддержка доступа к СКЗИ от прикладного ПО	Стандартный драйвер ОС Windows 2000/XP/2003/Vista/2008/Seven
Стандарт интерфейса подключения к ПЭВМ	USB 1.1
Тип USB порта	Тип А
Датчик случайных чисел (ДСЧ), тип	Программный
EEPROM память	64 Кбайт
Электропитание, В	+5
Внешние источники питания/батареи	Нет

Потребляемая мощность, Вт	0,12
Условия эксплуатации:	От +0° до +70° С От -10° до +80° С От 0 до 100% (без конденсата)
Габаритные размеры, мм	58x16x8
Масса, г	Не более 7

2.3. ПОКАЗАТЕЛИ НАДЕЖНОСТИ АППАРАТНОЙ ЧАСТИ ИЗДЕЛИЯ.

Гарантированное количество подключений к USB порту – до 5000.

2.4. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ ДЛЯ РАБОТЫ ИЗДЕЛИЯ

- IBM PC-совместимый компьютер с интерфейсом USB 1.1.
- Свободный USB порт типа А.
- Операционная система – Windows 2000/XP/2003/Vista/2008/Seven.

3. Комплектность

Обозначение изделия	Наименование изделия	Примечание
КБДЖ.468244.044 ФО	Формуляр	
КБДЖ.468244.044	Аппаратный модуль «РУТОКЕН ЭЦП»	Контрольная сумма микропрограммы AM – 0x04D1A287
КБДЖ.468244.044	СКЗИ «РУТОКЕН ЭЦП», Правила пользования	
КБДЖ.00050-0240	Дистрибутив «Стуртоп API, версия 2.4»	Контрольная сумма динамической библиотеки СтуртAPI.dll – 0x2100ACCE
КБДЖ.00179-0310	Дистрибутив «Драйвер «РУТОКЕН» для SC API, версия 3.1»	Контрольная сумма драйвера – 0xA6E61315
КБДЖ.00179-0310 34	Драйвер «РУТОКЕН» для SC API. Руководство пользователя	
КБДЖ.00182-0110	Дистрибутив «Драйвер шифрования «РУТОКЕН» для Стуртоп API, версия 1.1»	Контрольная сумма драйвера СтуртAPI.sys – 0xD848299F
КБДЖ.00182-0110 34	Драйвер шифрования «РУТОКЕН» для Стуртоп API. Руководство пользователя	
КБДЖ.00610-0100	Дистрибутив «Программный модуль АРМ ЭКИ «РУТОКЕН ЭЦП», версия 1.0»	Контрольная сумма исполняемого файла программного модуля

КБДЖ.00204-0240	Дистрибутив «Стуртон ArcMail, версия 2.4»	(ГЕСР_ARM.exe) – 0xDF0482E7
КБДЖ.00204-0240 34	Стуртон ArcMail. Руководство пользователя	Контрольная сумма динамической библиотеки ArcMainDll.dll – 0xD68F5D8A
КБДЖ.468243.028-01	Изделие "КРИПТОН-8S/PC"	
КБДЖ.468243.028-01 ФО	Изделие "КРИПТОН-8S/PC" формуляр	
КБДЖ.468243.024-04	Изделие "КРИПТОН-4S/PC"	
КБДЖ.468243.024-04 ФО	Изделие "КРИПТОН-4S/PC" формуляр	
КБДЖ.468243.039 / КБДЖ.468243.067	Изделие M-5265	
КБДЖ.468243.039 ФО/ КБДЖ.468243.067 ФО	Изделие M-5265	
КБДЖ.468244.046	АРМ ЭКИ «РУТОКЕН ЭЦП».	
КБДЖ.00610-0100 33	Руководство администратора АРМ «РУТОКЕН ЭЦП». Инструкция по встраиванию Упаковка	

Допускается поставка дистрибутивов программного обеспечения и документации на едином носителе типа CD или DVD.
Комплектность конкретного экземпляра СКЗИ может различаться в зависимости от типа поставки СКЗИ.

4. Свидетельство о приемке

Средство криптографической защиты информации «РУТОКЕН ЭЦП» КБДЖ.468244.044, исполнение ____, заводской номер см. Приложение №1. Соответствует техническим условиям КБДЖ.468244.044 ТУ приznание годным для эксплуатации.

Начальник ОТК _____
" 30 " сентя 2013 г.



5. Гарантийные обязательства

ЗАО «Актив-софт» гарантирует, что:

- Изделие прошло приемку, соответствует техническим условиям КБДЖ.468244.044 ТУ и признано годным к эксплуатации.
- Носитель дистрибутива программного обеспечения изделия не содержит производственных дефектов, влекущих его непригодность.

Никаких гарантий, кроме перечисленных выше, не предоставляется. ЗАО «Актив-софт» не несет ответственности за какой-либо ущерб (включая все, без исключения, случаи потери прибыли, прерывания деловой активности, потери деловой информации, либо других потерь), связанный с использованием или невозможностью использования изделия.

Гарантийный срок эксплуатации изделия – 12 месяцев с даты продажи. Гарантийный ремонт производится по предъявлении данного формуляра с отметкой о дате продажи. При отсутствии этой отметки срок гарантии исчисляется с даты приемки изделия изготовителем.

Заявки на гарантийный ремонт должны подаваться в письменной форме до истечения гарантийного срока и подтверждаться достаточными для ЗАО «Актив-софт» свидетельствами неисправности.

Гарантийный ремонт НЕ ПРОИЗВОДИТСЯ при явных механических повреждениях изделия или следах вмешательства в его электрическую схему.

Гарантийный срок хранения до ввода в эксплуатацию – 3 года.

Гарантийный ремонт и послегарантийное обслуживание осуществляется изготовителем по адресу:

Россия, 123056, Россия, г. Москва, ул. Красина, 3
Тел./Факс: (495) 925-77-90
E-mail: hotline@rutoken.ru

Примечание: доставка изделия ЗАО «Актив-софт» и обратно оплачивается потребителем.

Дополнительные услуги по установке, техническому обслуживанию, консультированию пользователей, сопровождению изделий и т. п. оказываются в порядке и на условиях, определяемых ЗАО «Актив-софт».

Установка и/или использование изделия означают согласие потребителя со всеми условиями, приведенными в данном разделе.

6. Отметка о продаже

Дата продажи: " 30 " сентя 2013 г.

Отгрузил _____ (подпись)





ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/121-2052 от "25" января 2012 г.

Действителен до "25" января 2016 г.

Выдан _____
закрытому акционерному обществу «Актив-софт»,
обществу с ограниченной ответственностью Фирма «АНКАД».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) «РУТОКЕН ЭИШ» в составе согласно формуляру КБДЖ.468244.044 ФО

соответствует Требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС2, и может использоваться для реализации функций электронной подписи (создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) и соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Сертификат выдан на основании результатов проведенных испытаний с ограниченной ответственностью «Центр сертификационных исследований» №.№. 388Э-001001, 388Э-001002.

Безопасность информации обеспечивается при использовании СКЗИ, изготовленного в соответствии с техническими условиями КБДЖ.468244.044 ТУ, выполнении требований нормативных документов формуляра КБДЖ.468244.044 ФО и сохранении в тайне ключей электронной подписи.



А.М.Ивашко

Заместитель руководителя Научно-технической
службы – начальник Центра защиты информации
и специальной связи ФСБ России

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию,
сертификации и защите государственной тайны ФСБ России

А.Н.Копылов

Приложение №1

792418644, 792420518, 792421017, 792421574, 792419013, 792418736,
792419061, 792420494, 792420970, 792420928, 792419008, 792420645,
792420069, 792421013, 792420026, 792420052, 792420947, 792419631,
792419661, 792420611, 792420033, 792421508, 792421531, 792420114,
792418986, 792421039, 792419096, 792419012, 792418989, 792419766,
792419629, 792420610, 792420588, 792421529, 792420997, 792421058,
792421460, 792418690, 792419314, 792419682, 792419634, 792420028,
792420032, 792421441, 792420901, 792421553, 792420900, 792419075,
792419401, 792419662, 792419681, 792419674, 792420498, 792420472,
792421506, 792420906, 792421597, 792419664, 792419383,
792419676, 792419659, 792421550, 792420903, 792420545, 792420605,
792421492, 792421555, 792421489, 792418785, 792419099, 792420480,
792420594, 792421440, 792421533, 792421012, 792419431, 792420089,
792419078, 792418766, 792418648, 792419097, 792418692, 792420595,
792420520, 792420973, 792421493, 792421041, 792420118, 792421577,
792421014, 792418812, 792419378, 792418740, 792418810, 792420495,
792420609, 792420992, 792421536, 792421579, 792419726, 792420055,
792419722, 792419362, 792420920, 792419357, 792421532, 792419271,
792418716, 792419004, 792419076, 792418786, 792418818, 792418817,
792419009, 792420003, 792420497, 792421528, 792420923, 792419331,
792421512, 792419285, 792419056, 792421556, 792418667, 792418768,
792420473, 792420613, 792420946, 792420969, 792418765, 792420142,
792420899, 792421557, 792420929, 792418963, 792420612, 792421494,
792421576, 792419010, 792418734, 792419788, 792418938, 792420589,
792419338, 792421063, 792420162, 792418813, 792421461, 792420995,
792419744, 792418763, 792419059, 792419029, 792419268, 792419336,
792421491, 792420592, 792421015, 792420160, 792421035, 792419382,
792418713, 792419101, 792418960, 792419079, 792419363, 792419746,
792421458, 792421511, 792420541, 792420138, 792421595, 792420161,
792419406, 792419427, 792419081, 792418697, 792419721, 792419703,
792421603, 792421445, 792420922, 792421061, 792420996, 792419425,
792418781, 792418714, 792418693, 792418735, 792419791, 792420522,
792421443, 792421437, 792421507, 792420164, 792421510, 792419751,
792418711, 792419426, 792418741, 792418779, 792420523, 792420591,
792421552, 792421442, 792421036, 792419403, 792420994, 792418819,
792418645, 792418739, 792420519, 792418984, 792419034, 792419789,
792419747, 792419632, 792420075, 792420004, 792420096, 792420029,
792419361, 792418671, 792419376, 792419058, 792418964, 792419794,
792419683, 792419663, 792420070, 792421011, 792419699, 792420157,

792419289, 792420027, 792418962, 792419062, 792419750, 792419748,
792420068, 792420057, 792420561, 792420140, 792421870, 792420968,
792420925, 792419266, 792421602, 792419100, 792418965, 792419335,
792419364, 792420115, 792420562, 792421888, 792420119, 792421867,
792420116, 792419310, 792418788, 792419032, 792419060, 792419793,
792419677, 792420539, 792420001, 792421866, 792420517, 792421871,
792420163, 792421601, 792419311, 792419030, 792419028, 792419675,
792419749, 792419430, 792420054, 792421869, 792420166, 792419399,
792419429, 792418787, 792419027, 792419080, 792419792, 792419337,
792420092, 792420007, 792421038, 792419360, 792421865, 792420090,
792418769, 792418767, 792418941, 792419665, 792421436, 792421885,
792420141, 792419407, 792418717, 792419267, 792418672, 792420646,
792419768, 792420971, 792421530, 792419291, 792420650, 792421040,
792420902, 792418642, 792418647, 792418646, 792419790, 792419725,
792418649, 792420113, 792420008, 792420949, 792419308, 792421065,
792420051, 792419405, 792420074, 792418712, 792418715, 792419628,
792420098, 792419288, 792419312, 792418737, 792418691, 792419724,
792419723, 792420496, 792420006, 792420972, 792420137, 792421037,
792420139, 792419313, 792419265, 792418694, 792418738, 792419700,
792418784, 792419720, 792420005, 792420540, 792421059, 792420165,
792421016, 792420948, 792419334, 792419332, 792418990, 792418944,
792419696, 792419765, 792420471, 792420002, 792420544, 792419745,
792420943, 792421018, 792421604, 792419290, 792418940, 792418937,
792419771, 792420053, 792420056, 792420985, 792420093,
792420564, 792420091, 792419680, 792419287, 792418985, 792419270,
792421596, 792418961, 792419635, 792419697, 792420050, 792420073,
792420944, 792419769, 792420988, 792419698, 792419269, 792421573,
792418939, 792419432, 792420071, 792421062, 792419702, 792418696,
792418720, 792419286, 792421509, 792418764, 792420924, 792420474,
792418816, 792418670, 792419365, 792418983, 792419005, 792419400,
792418987, 792419356, 792419630, 792420608, 792418669, 792418762,
792420136, 792420477, 792420993, 792419770, 792419077, 792420593,
792418988, 792420097, 792420475, 792421580, 792421554, 792419428,
792420967, 792420117, 792419333, 792418643, 792419033, 792419095,
792420590, 792420945, 792420547, 792421505, 792419377, 792421578,
792419380, 792418668, 792420524, 792418811, 792419094, 792420476,
792420563, 792421463, 792421462, 792421600, 792419719, 792419381,
792419011, 792419063, 792421444, 792421575, 792420647, 792419098,
792419057, 792420538, 792420500, 792421459, 792419315, 792421490,
792420905, 792419074, 792419031, 792420521, 792420651, 792421488,

792421487, 792420921, 792419264, 792419408, 792421527, 792420025,
792418695, 792418945, 792419633, 792418946, 792420120, 792419660,
792421064, 792420649, 792419379, 792420546, 792420499, 792419795,
792418780, 792421551