Токены с аппаратной поддержкой алгоритмов ГОСТ и действующим сертификатом ФСБ

Автор: Алексей Комаров (ZLONOV.ru)		*Дата актуализации: 31 октября 2016 г.*						
Название		**MS_KEY K**	**ESMART Token ГОСТ**	**eToken ГОСТ**	**JaCarta ГОСТ**		**РУТОКЕН ЭЦП**	**РУТОКЕН ЭЦП 2.0**
Производитель(и)		ООО МультиСофт Системз NXP Semiconductors N.V.	ОАО «НИИМЭ и завод Микрон» ООО «ИСУБ» (ISBC group)	ЗАО «АЛАДДИН Р.Д.» SafeNet (Gemalto)	ЗАО «АЛАДДИН Р.Д.» Athena SCS Limited NXP Semiconductors N.V.		ЗАО «Актив-софт» ООО Фирма «Анкад»	
Сертификат ФСБ		СФ/124-2673	СФ/124-2772	СФ/111-2750	СФ/124-2963		СФ/124-2846 / СФ/124-2847 / СФ/124-2848	СФ/124-2771
от		30.07.15	25.12.15	1.12.15	09.09.16		01.02.16	25.12.15
до		01.08.18	25.12.18	1.12.18	31.12.18		31.12.18	25.12.18
на что выдан		устройство MS_KEY K	микросхема MIK51	Криптотокен ЭП	Криптотокен 2		устройство РУТОКЕН ЭЦП	устройство РУТОКЕН ЭЦП 2.0
класс		КС1 / КС2	КС3	КС1 / КС2			КС1, КС2	КС1 / КС2
наименование изделия		MS_KEY K (варианты исполнения 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.2.4)	Отечественная микросхема MIK51SC72Dv6 с операционной системой Trust 2.05, предназначенная для использования в качестве средства криптографической защиты информации	изделие «Персональное средство электронной подписи «Криптотокен ЭП» (исполнения 1, 2) в комплектации согласно формуляру 46538383.50 1430 007-01 30 01-1, предназначенное для использования совместно со Средством криптографической защиты информации «Криптотокен» в составе изделия «JaCarta ГОСТ» («eToken ГОСТ»)	изделие «Средство криптографической защиты информации «Криптотокен 2» в составе изделия JaCarta ГОСТ» (варианты исполнения 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)		РУТОКЕН ЭЦП (исполнение 1: РУТОКЕН ЭЦП) / РУТОКЕН ЭЦП (исполнение 2: РУТОКЕН ЭЦП micro) / РУТОКЕН ЭЦП (исполнение 3: РУТОКЕН ЭЦП Flash)	средство криптографической защиты информации (СКЗИ) Рутокен ЭЦП 2.0 (исполнения 1,2)
чему соответствует		соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 и требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС1 (для вариантов исполнения 5.1.2, 5.2.2), класса КС2 (для вариантов исполнения 5.1.1, 5.1.3, 5.2.1, 5.2.3, 5.2.4), Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для вариантов исполнения 5.1.2, 5.2.2), класса КС2 (для вариантов исполнения 5.1.1, 5.1.3, 5.2.1, 5.2.3, 5.2.4), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование данных, содержащихся в областях оперативной памяти СКЗИ, вычисление имитовставки для данных, содержащихся в областях оперативной памяти СКЗИ, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти СКЗИ, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну	соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 и требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС3 и может использоваться для криптографической защиты (шифрование данных, содержащихся в оперативной памяти изделия, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти изделия, создание и проверка электронной подписи для данных, содержащихся в оперативной памяти изделия) информации, не содержащей сведений, составляющих государственную тайну	соответствует Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для исполнения 1) и класса КС2 (для исполнения 2), и может использоваться для реализации функций электронной подписи (создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»	соответствует Требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012, Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для вариантов исполнения 1, 2, 3, 7, 9, 11) и класса КС2 (для вариантов исполнения 4, 5, 6, 8, 10, 12) и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование данных, содержащихся в областях оперативной памяти, вычисление имитовставки для данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти, создание и проверка электронной подписи для данных, содержащихся в областях оперативной памяти) информации, не содержащей сведений, составляющих государственную тайну.		соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, классов КС1, КС2, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для классов КС1, КС2, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование данных, содержащихся в областях оперативной памяти СКЗИ, вычисление имитовставки для данных, содержащихся в областях оперативной памяти СКЗИ, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти СКЗИ, создание и проверка электронной подписи для данных, содержащихся в областях оперативной памяти СКЗИ, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну	соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения 1) и класса КС2 (для исполнения 2), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование данных, содержащихся в областях оперативной памяти СКЗИ, вычисление имитовставки для данных, содержащихся в областях оперативной памяти СКЗИ, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти СКЗИ, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну
Микросхема смарт-карты		защищенный смарт-карточный чип от NXP	Отечественная микросхема MIK51SC72Dv6 (Микрон)	Atmel AT90SC25672RCT со встроенными контроллерами ISO 7816 (для смарт-карт) или USB 2.0 (для USB-ключей)	Защищённый смарт-карточный чип AT90SC25672RCT либо AT90SC28880RCV, имеющий специальную сертифицированную защиту и на аппаратном, и на программном уровне	Защищённый смарт-карточный чип AT90SC28880RCV, имеющий специальную сертифицированную защиту и на аппаратном, и на программном уровне	защищенный микроконтроллер со встроенной энергонезависимой памятью	защищенный 32-разрядный микроконтроллер архитектуры ARM7 со встроенной энергонезависимой памятью
Операционная система смарт-карты		н/д	Операционная система Trust 2.05	Athena OS755, встроенная виртуальная машина Java (полностью совместимая со стандартами Java Card Platform Specification 2.2.2 и Global Platform 2.1.1)	Athena OS755		Операционная система Рутокен	Операционная система Рутокен
Поддерживаемые интерфейсы и стандарты		PKCS#11 v2.30, APDU (ISO7816), Microsoft CryptoAPI, Веб-криптоплагин Netscape Plugin API (NPAPI), Веб-криптоплагин ActiveX, JCA (Java Cryptography Architecture), Интерфейс подключаемых модулей (engine) OpenSSL 1.0.0; NSS (Network Security Services)	PKCS#11 версии 2.30, Microsoft CryptoAPI PC/SC, Microsoft CCID, Сертификаты X.509 v3, SSL v3, IPSec/IKE, ISO 7816 части 1, 2, 3, 4, 8, 9, ISO 14443 части 1, 2, 3, 4	PKCS#11 версии 2.30, Microsoft CryptoAPI, PC/SC, Сертификаты X.509 v3, SSL v3, IPSec/IKE, Microsoft CCID, APDU, Криптотокен ЭП, JC-WebClient, файловая система etFS/jcFS.	APDU, PC/SC, PKCS #11 2.30, MS CAPI (CSP, CNG), Microsoft CCID, Сертификаты X.509, SSL v3, IPSec/IKE, JC-WebClient, jcFS, Криптотокен ЭП, Криптотокен 2.		Протокол обмена по ISO 7816-12, Поддержка USB CCID: работа без установки драйверов устройства в современных версиях ОС, Поддержка PC/SC, Microsoft Crypto API, Microsoft SmartCard API, PKCS#11 (включая российский профиль), физический интерфейс ISO/IEC 7816-3, протокол T=0 (для смарт-карт)	Протокол обмена по ISO 7816-12, Поддержка USB CCID: работа без установки драйверов устройства в современных версиях ОС, Поддержка PC/SC, Microsoft Crypto API, Microsoft SmartCard API,PKCS#11 (включая российский профиль).
Аппаратно-реализованные алгоритмы	**Алгоритмы вычисления/ проверки электронной подписи**	ГОСТ Р 34.10-2001 RSA-1024	ГОСТ Р34.10-2001, ГОСТ Р 34.10-2012, RSA-1024, RSA-2048, ECDSA-256	ГОСТ Р 34.10-2001	ГОСТ Р 34.10-2001, для комбинированных моделей RSA 1024, 2048 ECDSA 256.	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012. Для комбинированных моделей RSA 1024, 2048 ECDSA 256.	ГОСТ Р 34.10-2001 RSA-2048	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 RSA-2048
	Алгоритмы шифрования	ГОСТ 28147-89 DES/3DES, AES	ГОСТ 28147-89, DES, Triple DES, AES-128, AES-192, AES-256	ГОСТ 28147-89 (не сертифицирован)	ГОСТ 28147-89 (не сертифицирован)	ГОСТ 28147-89	ГОСТ 28147-89	ГОСТ 28147-89
	Алгоритмы хеширования	ГОСТ Р 34.11-94 SHA-1	ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 SHA-1, SHA-256	ГОСТ Р 34.11-94	ГОСТ Р 34.11-94	ГОСТ Р 34.11-94 ГОСТ Р 34.11-2012	ГОСТ Р 34.11-94	ГОСТ Р 34.11-94 ГОСТ Р 34.11-2012
	Генератор случайных чисел	генерация случайных последовательностей произвольной длины с помощью программного датчика случайных чисел	Есть	генерация последовательности случайных чисел	генератор последовательностей случайных чисел		Сертифицированный ДСЧ	Сертифицированный ДСЧ
	Дополнительно		Выработка сессионных ключей по схеме VKO GOST R 34.10-2001 (RFC4357) и VKO GOST R34.10-2012 (RFC 7836, Протокол ТК 26 №13 от 24.04.2014 г.)	Выработка ключа парной связи по алгоритму Диффи-Хеллмана согласно RFC 4357	алгоритм Диффи-Хеллмана (выработка ключа парной связи в соответствии с RFC 4357);		Выработка сессионных ключей (ключей парной связи): по схеме VKO GOST R 34.10-2001 (RFC 4357), расшифрование по схеме EC El-Gamal.	Выработка сессионных ключей (ключей парной связи): по схеме VKO GOST R 34.10-2001 (RFC 4357) и VKO GOST R 34.10-2012 (RFC 7836, Протокол ТК 26 №13 от 24.04.2014 г.), расшифрование по схеме EC El-Gamal.
Скорость работы		н/д	Время вычисления/проверки ЭП ГОСТ - 90 мс / 173 мс	н/д	н/д		Скорость хеширования ГОСТ Р 34.11-94: до 61 КБ/сек. Скорость шифрования ГОСТ 28147-89: до 91 КБ/сек.	Скорость хеширования ГОСТ Р 34.11-94: до 61 КБ/сек. Скорость хеширования ГОСТ Р 34.11-2012: до 61 КБ/сек. Скорость шифрования ГОСТ 28147-89: до 91 КБ/сек.
Объем защищенной памяти		80Кб	72 Кбайт (весь объем памяти доступен для пользовательских данных)	72 КБ на микросхеме смарт-карты	72 КБ (для хранения пользовательских данных доступно ~29 КБ)	80 КБ EEPROM	64 Кбайт	64 Кбайт
Модели		смарт-карта USB-токен	смарт-карта USB-токен	смарт-карта USB-ключ USB-ключ с дополнительным модулем Flash-памяти USB-ключ с генератором одноразовых паролей	смарт-карта USB-ключ USB-ключ с дополнительным модулем Flash-памяти MicroUSB Secure MicroSD		смарт-карта USB-ключ USB-ключ micro USB-ключ с дополнительным модулем Flash-памяти	USB-ключ USB-ключ micro USB-ключ с дополнительным модулем Flash-памяти
Возможность встраивания радио-метки (RFID)		н/д	есть: EM-Marine, Mifare, ICODE, HID Prox, HID Indala, HID iClass	есть	есть: EM-Marine, HID, Indala, Mifare, Ангстрем		есть: EM-Marine, Mifare, ProxCard II, ISOProx II, Indala (на заказ)	есть: EM-Marine, Mifare, ProxCard II, ISOProx II, Indala (на заказ)
Поддерживаемые операционные системы	**Microsoft**	Microsoft Windows XP/7 (32/64-бит)	Microsoft Windows XP/2003/Vista/2008/7/8 (32/64-бит) Microsoft Windows 10	Windows XP/2003/Vista/2008/7 (32/64-бит)	Microsoft Windows XP SP2 (x64) XP SP3 (x32) Vista SP2/7/8 (x32/x64) Server 2003 SP2 (x32/x64) Server 2008 (x32/x64) Server 2008 R2 Server 2012 (x32/x64)	Microsoft Windows XP SP2 (x64) XP SP3 (x32) Vista SP2/7/8/8.1 (x32/x64) Server 2003 SP2 (x32/x64) Server 2008 (x32/x64) Server 2008 R2 Server 2012 (x32/x64)	Windows 10/8.1/8/2012/7/2008/Vista/2003/XP	Windows 10/8.1/8/2012/7/2008/Vista/2003/XP
	MacOS	н/д	MacOS X	MacOS X (RISC, Intel)	нет	10.10 Yosemite 10.11 El Capitan	Apple Mac OS X / OS X	Apple Mac OS 10.6/10.7/10.8/10.9/10.10
	Linux	н/д	Linux	SuSE, RedHat, Ubuntu	LSB 3.1	ОС, соответствующие спецификациям Linux Standard Base 4.0 (IA-32, AMD64): Mandriva Enterprise Server 5; Oracle Linux 5 Update 5; Oracle Linux 5 Update 6; Oracle Linux 6; Red Hat Enterprise Linux 5.6; Red Hat Enterprise Linux 6.0; SUSE Linux Enterprise Server 11 SP4; ОС, соответствующие спецификациям Linux Standard Base 4.1 (IA-32, AMD64): Red Hat Enterprise Linux 7.0; Astra Linux Common Edition; Astra Linux Special Edition; CentOS 7; Debian 8.4; openSUSE 13.2; openSUSE Leap 42.1; Ubuntu 14.04; Red Hat Enterprise Linux 7.2; ROSA Enterprise Desktop X1 (Marathon); ROSA Enterprise Linux Server; МСВС 3.0; МСВС 5.0; МСВСфера; Ред ОС; РОСА DX «КОБАЛЬТ» 1.0; РОСА SX «КОБАЛЬТ» 1.0.	GNU/Linux	LSB 4.0; Ubuntu 10.10 / 11.04 / 11.10 / 12.04 / 12.10 / 13.04 / 13.10 / 14.04; Debian 6.0 / 7; RHEL 4 / 5 / 6 / 7; Fedora 12 / 13 / 14 / 15/ 16 / 17 / 18 / 19 / 20; CentOS 5 / 6 / 7; ALTLinux 6 / 7; Oracle Enterprise Linux 5 / 6 / 7; OpenSUSE 11.4 / 12.2 / 12.3 / 13.1; SUSE Linux Enterprise 11; Astra Linux 1.2, 1.3, 1.4, 1.5, 1.7, 1.9, 1.10, 1.11 ОС FreeBSD

Поддержка ГОСТ алгоритмов и особенности сертификации токенов с действующими сертификатами ФСБ

Токен	Сертификат	На что выдан сертификат	Электронная подпись			Шифрование	Хеширование	
			Приказ ФСБ № 796 и Федеральный закон № 63-ФЗ	ГОСТ Р34.10-2001	ГОСТ Р 34.10-2012	ГОСТ 28147-89	ГОСТ Р 34.11-94	ГОСТ Р 34.11-2012
MS_KEY K	**СФ/124-2673 до 01.08.18**	устройство MS_KEY K						
ESMART Token ГОСТ	**СФ/124-2772 до 25.12.18**	микросхема MIK51						
eToken ГОСТ	**СФ/111-2750 до 01.12.18**	Криптотокен ЭП						
JaCarta ГОСТ	**СФ/111-2750 до 01.12.18**	Криптотокен ЭП						
	СФ/124-2963 до 31.12.18	Криптотокен 2						
РУТОКЕН ЭЦП	**СФ/124-2846, СФ/124-2847, СФ/124-2848 до 31.12.18**	устройство РУТОКЕН ЭЦП						
РУТОКЕН ЭЦП 2.0	**СФ/124-2771 до 25.12.18**	устройство РУТОКЕН ЭЦП 2.0						

Автор: Алексей Комаров (ZLONOV.ru) *Дата актуализации: 31 октября 2016 г.*

Обозначения:	сертифицировано	реализовано, но не сертифицировано	не реализовано