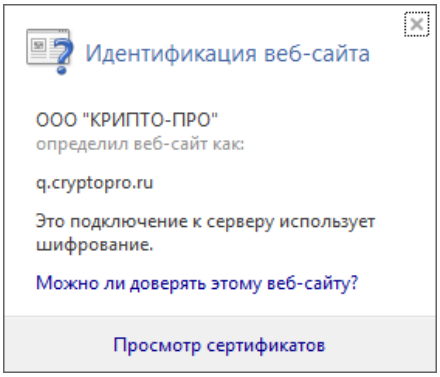
ИЗВЕЩЕНИЕ ОБ ИЗМЕНЕНИЯХ

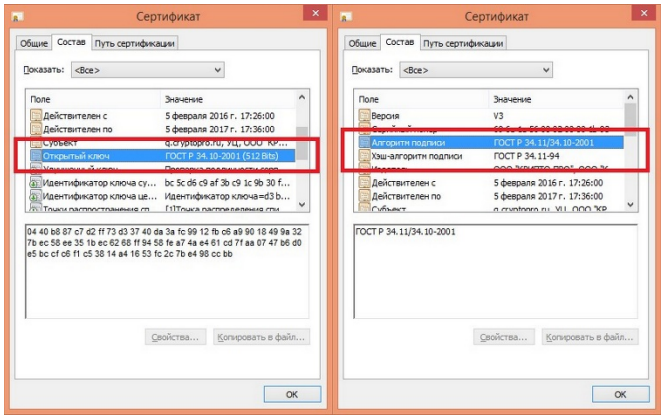
ООО «КРИПТО-ПРО»	ОТД	ИЗВЕЩЕНИЕ			ОБОЗНАЧЕНИЕ	
	ОЛС	ЖТЯИ.00087-01.1-2016			ЖТЯИ.00087-01	
ДАТА ВЫПУСКА		СРОК ИЗМЕНЕНИЯ			Лист	Листов
06.09.2016		С момента утверждения извещения об изменениях ЖТЯИ.00087-01			1	11
ПРИЧИНА		Изменение списка поддерживаемых программно-аппаратных средств			КОД 3	
УКАЗАНИЯ О ЗАДЕЛЕ		Не отражается				
УКАЗАНИЯ О ВНЕДРЕНИИ		После проведения контроля				
ПРИМЕНЯЕМОСТЬ		ЖТЯИ.00087-01				
РАЗОСЛАТЬ		ФСБ России, ООО «ЦСИ», ООО «КРИПТО-ПРО»				
ПРИЛОЖЕНИЕ		ЖТЯИ.00087-01 91 09. Руководство администратора безопасности. Виртуальные среды				

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
1	Изменен список поддерживаемых программно-аппаратных сред. Соответствующие изменения внесены в следующие документы: ЖТЯИ.00087-01 30 01. Формуляр; ЖТЯИ.00087-01 90 01. Описание реализации; ЖТЯИ.00087-01 91 01. Руководство администратора безопасности. Общая часть; ЖТЯИ.00087-01 93 01. Приложение командной строки для подписи и шифрования файлов; ЖТЯИ.00087-01 93 02. Приложение командной строки для работы с сертификатами; ЖТЯИ.00087-01 93 03. Приложение для создания TLS-туннеля; ЖТЯИ.00087-01 95 01. Правила пользования. Старая редакция: «Windows 7/8/8.1/Server 2003/2008 (x86, x64); Windows Server 2008 R2/2012/2012 R2 (x64). CentOS 4/5/6/7 (x86, x64, POWER, ARM); ТД ОС АИС ФССП России (GosLinux) (x86, x64); Red OS (x86, x64); Fedora 19/20 (x86, x64, ARM); Mandriva Enterprise Server 5, Business Server 1 (x86, x64, ARM); Oracle Linux 4/5/6/7 (x86, x64); OpenSUSE 13.2, Leap 42 (x86, x64, ARM); SUSE Linux Enterprise Server 11SP4/12, Desktop 12 (x86, x64, POWER, ARM); Red Hat Enterprise Linux 4/5/6/7 (x86, x64, POWER, ARM); Синтез-ОС.РС (x86, x64, POWER, ARM); Ubuntu 10.04/12.04/12.10/13.04/14.04/14.10 (x86, x64, POWER, ARM); Linux Mint 13/14/15/16/17 (x86, x64); Debian 7/8 (x86, x64, POWER, ARM); Astra Linux Special Edition (x86-64). ALT Linux 7 (x86, x64, ARM); ROSA 2011, Enterprise Desktop X.1 (Marathon), Enterprise Linux Server (x86, x64); РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64); FreeBSD 9, pfSense 2.x (x86, x64); AIX 5/6/7 (POWER); Mac OS X 10.7/10.8/10.9/10.10/10.11 (x64). Solaris 10 (sparc, x86, x64); Solaris 11 (sparc, x64). Apple iOS 6.0/6.0.1/6.0.2/6.1/6.1.2/6.1.3/6.1.4/6.1.5/6.1.6/7.0/7.0.1/7.0.2/7.0.3/7.0.4/7.0.5/7.0.6/7.1/7.1.1/7.1.2/8.0/8.0.1/8.0.2/8.1/8.1.1/8.1.2/8.1.3/8.2/8.3/8.4/8.4.1/9/9.0.1/9.0.2/9.1/9.2/9.2.1 (ARM, arm64, arm7s).»

СОСТАВИЛ	МОШНИНА Д.А.			Н.КОНТРОЛЬ		
ИЗМЕНЕНИЕ ВНЕС				МОШНИНА Д.А. 06.09.2016		

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
1	Новая редакция: «Windows 7/8/8.1/10/Server 2003/2008 (x86, x64); Windows Server 2008 R2/2012/2012 R2/2016 (x64). CentOS 4/5/6/7 (x86, x64, POWER, ARM); ТД ОС АИС ФССП России (GosLinux) (x86, x64); Red OS (x86, x64); Fedora 23/24/25 (x86, x64, ARM); Mandriva Enterprise Server 5, Business Server 1 (x86, x64, ARM); Oracle Linux 4/5/6/7 (x86, x64); OpenSUSE 13.2, Leap 42 (x86, x64, ARM); SUSE Linux Enterprise Server 11SP4/12, Desktop 12 (x86, x64, POWER, ARM); Red Hat Enterprise Linux 4/5/6/7 (x86, x64, POWER, ARM); Синтез-ОС.РС (x86, x64, POWER, ARM); Ubuntu 10.04/12.04/12.10/13.04/14.04/14.10/15.04/15.10/16.04/16.04.1/16.10 (x86, x64, POWER, ARM); Linux Mint 13/14/15/16/17/18 (x86, x64); Debian 7/8 (x86, x64, POWER, ARM, MIPS); Astra Linux Special Edition (x86-64). ALT Linux 7 (x86, x64, ARM); ROSA 2011, Enterprise Desktop X.1 (Marathon), Enterprise Linux Server (x86, x64); РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64); FreeBSD 9/10, pfSense 2.x (x86, x64); AIX 5/6/7 (POWER); Mac OS X 10.7/10.8/10.9/10.10/10.11/10.12 (x64). Solaris 10 (sparc, x86, x64); Solaris 11 (sparc, x64). Apple iOS 6.0/6.0.1/6.0.2/6.1/6.1.2/6.1.3/6.1.4/6.1.5/6.1.6/7.0/7.0.1/7.0.2/7.0.3/7.0.4/7.0.5/7.0.6/7.1/7.1.1/7.1.2/8.0/8.0.1/8.0.2/8.1/8.1.1/8.1.2/8.1.3/8.2/8.3/8.4/8.4.1/9/9.0.1/9.0.2/9.1/9.2/9.2.1/9.3/9.3.1/9.3.2/9.3.3/9.3.4/9.3.5/10 (ARM, arm64, arm7s).» Добавлено:«Виртуальные среды Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016 (x64); VMWare WorkStation 11/12 (x86-64); VMWare Player 7/12 (x86, x64); VMWare Sphere ESXi 5.5/6.0 (x64); Virtual Box 3.2/4.0/4.1/4.2/4.3/5.0/5.1 (x86, x64); RHEV 3.4/3.5/3.6/4.0 (x64).» Следующие изменения внесены в документы: ЖТЯИ.00087-01 91 02. Руководство администратора безопасности. Windows. и ЖТЯИ.00087-01 94 01. АРМ выработки внешней гаммы. Старая редакция: «Windows 7/8/8.1/Server 2003/2008 (x86, x64); Windows Server 2008 R2/2012/2012 R2 (x64).» Новая редакция: «Windows 7/8/8.1/10/Server 2003/2008 (x86, x64); Windows Server 2008 R2/2012/2012 R2/2016 (x64).» Следующие изменения внесены в документ: ЖТЯИ.00087-01 91 04. Руководство администратора безопасности. FreeBSD. Старая редакция: «FreeBSD 9, pfSense 2.x (x86, x64)…pkg_add <файл_пакета>…pkg_delete <имя_пакета>…» Новая редакция: «FreeBSD 9/10, pfSense 2.x (x86, x64)…pkg_add <файл_пакета> (pkg add <файл_пакета> для FreeBSD 10)…pkg_delete <имя_пакета> (pkg delete <файл_пакета> для FreeBSD 10)…» Следующие изменения внесены в документ: ЖТЯИ.00087-01 91 03. Руководство администратора безопасности. Linux Старая редакция: «CentOS 4/5/6/7 (x86, x64, POWER, ARM); ТД ОС АИС ФССП России (GosLinux) (x86, x64); Red OS (x86, x64); Fedora 19/20 (x86, x64, ARM); Mandriva Enterprise Server 5, Business Server 1 (x86, x64, ARM); Oracle Linux 4/5/6/7 (x86, x64); OpenSUSE 13.2, Leap 42 (x86, x64, ARM); SUSE Linux Enterprise Server 11SP4/12, Desktop 12 (x86, x64, POWER, ARM); Red Hat Enterprise Linux 4/5/6/7 (x86, x64, POWER, ARM); Синтез-ОС.РС (x86, x64, POWER, ARM); Ubuntu 10.04/12.04/12.10/13.04/14.04/14.10 (x86, x64, POWER, ARM); Linux Mint 13/14/15/16/17 (x86, x64); Debian 7/8 (x86, x64, POWER, ARM); Astra Linux Special Edition (x86-64).» Новая редакция: «CentOS 4/5/6/7 (x86, x64, POWER, ARM); ТД ОС АИС ФССП России (GosLinux) (x86, x64); Red OS (x86, x64); Fedora 23/24/25 (x86, x64, ARM); Mandriva Enterprise Server 5, Business Server 1 (x86, x64, ARM); Oracle Linux 4/5/6/7 (x86, x64); OpenSUSE 13.2, Leap 42 (x86, x64, ARM); SUSE Linux Enterprise Server 11SP4/12, Desktop 12 (x86, x64, POWER, ARM); Red Hat Enterprise Linux 4/5/6/7 (x86, x64, POWER, ARM); Синтез-ОС.РС (x86, x64, POWER, ARM); Ubuntu 10.04/12.04/12.10/13.04/14.04/14.10/15.04/ 15.10/16.04/16.04.1/16.10 (x86, x64, POWER, ARM); Linux Mint 13/14/15/16/17/18 (x86, x64); Debian 7/8 (x86, x64, POWER, ARM, MIPS); Astra Linux Special Edition (x86-64).»

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
1	Следующие изменения внесены в документ ЖТЯИ.00087-01 91 08. Руководство администратора безопасности. iOS. Старая редакция: «СКЗИ «КриптоПро CSP» v 4.0 под управлением iOS используется в программно-аппаратных средах iOS версии 6.0, 6.0.1, 6.0.2, 6.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5, 6.1.6, 7.0, 7.0.1, 7.0.2, 7.0.3, 7.0.4, 7.0.5, 7.0.6, 7.1, 7.1.1, 7.1.2, 8.0, 8.0.1, 8.0.2, 8.1, 8.1.1, 8.1.2, 8.1.3, 8.2, 8.3, 8.4, 8.4.1, 9, 9.0.1, 9.0.2, 9.1, 9.2, 9.2.1.» Новая редакция: «СКЗИ «КриптоПро CSP» v 4.0 под управлением iOS используется в программно-аппаратных средах iOS версии 6.0, 6.0.1, 6.0.2, 6.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5, 6.1.6, 7.0, 7.0.1, 7.0.2, 7.0.3, 7.0.4, 7.0.5, 7.0.6, 7.1, 7.1.1, 7.1.2, 8.0, 8.0.1, 8.0.2, 8.1, 8.1.1, 8.1.2, 8.1.3, 8.2, 8.3, 8.4, 8.4.1, 9, 9.0.1, 9.0.2, 9.1, 9.2, 9.2.1, 9.3, 9.3.1, 9.3.2, 9.3.3, 9.3.4, 9.3.5, 10.» Добавлен новый документ ЖТЯИ.00087-01 91 09. Руководство администратора безопасности. Использование СКЗИ в виртуальных средах. (см. Приложение). Следующие изменения внесены в документ ЖТЯИ.00087-01 91 07. Руководство администратора безопасности. Mac OS. Старая редакция: «Mac OS X 10.7/10.8/10.9/10.10/10.11 (x64).» Новая редакция: «Mac OS X 10.7/10.8/10.9/10.10/10.11/10.12 (x64).»
2	В документ «ЖТЯИ.00087-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть» добавлено: 7.3 Проверка использования российских алгоритмов в браузере Internet Explorer/Edge. 1. Откройте браузер Internet Explorer/Edge. При посещении веб-страницы обратите внимание, используется ли протокол соединения «https».  Рисунок 7.3 – Адресная строка Internet Explorer. 2. Нажмите на значок «замка».  Рисунок 7.4 – Адресная строка Internet Explorer. Должно появится окно следующего вида:  Рисунок 7.5 – Окно идентификации Веб-сайта.

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
2	3. Нажмите на Просмотр сертификатов. Откроется SSL сертификат web-сервера. На вкладке «Состав» можно посмотреть информацию об используемых криптографических алгоритмах.  Рисунок 7.6 – Сертификат.
3	Добавлена поддержка Microsoft Edge. В следующую документацию внесены соответствующие изменения: ЖТЯИ.00087-01 90 01. Описание реализации ЖТЯИ.00087-01 91 01. Руководство администратора безопасности. Общая часть ЖТЯИ.00087-01 91 02. Руководство администратора безопасности. Windows Старая редакция: «…Internet Explorer…». Новая редакция: «…Internet Explorer/ Microsoft Edge …». В п. 2 документа ЖТЯИ.00087-01 95 01. Правила пользования добавлено: «… Необходимость проведения оценки влияния для прочих программных продуктов (в том числе установленных администратором/пользователем дополнений и расширений программного обеспечения, перечисленного выше) определяется с учетом п.1.5 Формуляра ЖТЯИ.00087-01 30 01…»
4	Расширен перечень вызовов, использование которых при разработке систем на основе СКЗИ «КриптоПро CSP» версии 4.0 возможно без дополнительных тематических исследований. В документ ЖТЯИ.00087-01 95 01. Правила пользования добавлено:

Дополнительные функции		
CryptBinaryToString	Функция переводит двоичную строку в строку Base64/HEX.	
CryptStringToBinary	Функция переводит строку Base64/HEX в двоичную строку.	

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ

4

CertFindAttribute	Функция производит поиск атрибута сертификата по идентификатору.	
CertGetNameString	Функция получает имя владельца или издателя сертификата.	
CertNameToStr	Функция производит раскодирование имени из ASN структуры в DN (RFC1779).	
CertSaveStore	Функция производит запись хранилища сертификатов (включая списки отозванных и доверенных сертификатов) в виде структуры PKCS#7 или бинарного дампа в память или файл.	
CryptFindCertificateKeyProvInfo	Функция осуществляет поиск закрытого ключа, соответствующего открытому ключу сертификата.	
CryptHashPublicKeyInfo	Функция осуществляет ASN1 кодирование и хэширование структуры CERT_PUBLIC_KEY_INFO.	
CryptMsgCountersign	Функция вырабатывает добавочную подпись.	
CryptMsgCountersignEncoded	Функция вырабатывает добавочную подпись (кодирует структуру SignerInfo, как определено в PKCS #7).	
CryptMsgVerifyCountersignatureEncoded	Функция проверяет добавочную подпись (декодирует структуру SignerInfo, как определено в PKCS #7).	
CryptMsgVerifyCountersignatureEncodedEx	Функция проверяет добавочную подпись (декодирует структуру SignerInfo, как определено в PKCS #7).	

Новая редакция:

CryptCreateHash	Функция CryptCreateHash инициализирует дескриптор нового объекта функции хэширования потока данных.	Разрешено использование только со следующими символьными аргументами: CALG_GR3411, CALG_GR3411_2012_256, CALG_GR3411_2012_512, CALG_GR3411_HMAC, CALG_GR3411_2012_256_HMAC, CALG_GR3411_2012_512_HMAC, CALG_SHAREDKEY_HASH.

5

Расширен список поддерживаемых архитектур. Добавлена поддержка архитектуры MIPS. В следующую документацию внесены соответствующие изменения:
ЖТЯИ.00087-01 30 01. Формуляр
ЖТЯИ.00087-01 90 01. Описание реализации
ЖТЯИ.00087-01 91 01. Руководство администратора безопасности. Общая часть
ЖТЯИ.00087-01 91 03. Руководство администратора безопасности. Linux
ЖТЯИ.00087-01 93 01. Приложение командной строки для подписи и шифрования файлов
ЖТЯИ.00087-01 93 02. Приложение командной строки для работы с сертификатами

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
5	ЖТЯИ.00087-01 93 03. Приложение для создания TLS-туннеля ЖТЯИ.00087-01 95 01. Правила пользования Старая редакция: «…Debian 7/8 (x86, x64, POWER, ARM);…» Новая редакция: «…Debian 7/8 (x86, x64, POWER, ARM, MIPS);…»
6	В документ ЖТЯИ.00087-01 95 01. Правила пользования внесены следующие изменения: Старая редакция: «…Разработка программного обеспечения на основе СКЗИ «КриптоПро CSP» может производиться без создания новых СКЗИ в случае использования вызовов из перечня Приложения 2. ...Приложение 2. Перечень вызовов, использование которых при разработке систем на основе СКЗИ «КриптоПро CSP» возможно без дополнительных тематических исследований:…» Новая редакция: «…Разработка программного обеспечения на основе СКЗИ «КриптоПро CSP» с учетом п.1.5 Формуляра ЖТЯИ.00087-01 30 01 может производиться без создания новых СКЗИ в случае использования вызовов из перечня Приложения 2. … Приложение 2. Перечень вызовов, использование которых при разработке систем на основе СКЗИ «КриптоПро CSP» с учетом п.1.5 Формуляра ЖТЯИ.00087-01 30 01 возможно без дополнительных тематических исследований:…»
7	В документе ЖТЯИ.00087-01 91 02. Руководство администратора безопасности. Windows скорректирован список системных библиотек, находящихся под контролем целостности. Добавлены библиотеки, перечисленные ниже. Новая редакция: «…**Windows 32-bit** … \Windows\system32\inetcomm.dll \Windows\system32\rastls.dll \Windows\system32\wininet.dll \Windows\system32\msi.dll \Windows\system32\crypt32.dll \Windows\system32\schannel.dll \Windows\system32\kerberos.dll \Windows\system32\certenroll.dll \Windows\system32\cryptsp.dll* \Windows\system32\sspicli.dll* * Для ОС Windows Server 2008 под контролем целостности вместо библиотек cryptsp.dll и sspicli.dll находятся библиотеки \Windows\system32\advapi32.dll и \Windows\system32\secur32.dll **Windows 64-bit** … \Windows\system32\inetcomm.dll \Windows\SysWOW64\inetcomm.dll \Windows\system32\rastls.dll \Windows\SysWOW64\rastls.dll \Windows\system32\wininet.dll

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
7	\Windows\SysWOW64\wininet.dll \Windows\system32\msi.dll \Windows\SysWOW64\msi.dll \Windows\system32\crypt32.dll \Windows\SysWOW64\crypt32.dll \Windows\system32\schannel.dll \Windows\SysWOW64\schannel.dll \Windows\system32\kerberos.dll \Windows\SysWOW64\kerberos.dll \Windows\system32\certenroll.dll \Windows\SysWOW64\certenroll.dll \Windows\system32\cryptsp.dll* \Windows\SysWOW64\cryptsp.dll* \Windows\system32\sspicli.dll* \Windows\SysWOW64\sspicli.dll* * Для ОС Windows Server 2008 под контролем целостности вместо библиотек cryptsp.dll и sspicli.dll находятся библиотеки \Windows\system32\advapi32.dll \Windows\SysWOW64\advapi32.dll \Windows\system32\secur32.dll \Windows\SysWOW64\secur32.dll В случае если целостность данных библиотек нарушена в результате обновления операционной системы, необходимо обратиться к разработчику СКЗИ за разъяснениями о возможности продолжения использования СКЗИ на данной системе.»
8	В документах ЖТЯИ.00087-01 91 01. Руководство администратора безопасности. Общая часть и ЖТЯИ.00087-01 95 01. Правила пользования удалено: «…исключение: дистрибутивы на ОС Windows дополнительно содержат в себе значение подписи в формате Microsoft Authenticode…»
9	В следующие документы внесены изменения порядка контроля действия ключей: ЖТЯИ.00087-01 91 01. Руководство администратора безопасности. Общая часть ЖТЯИ.00087-01 91 02. Руководство администратора безопасности. Windows ЖТЯИ.00087-01 91 03. Руководство администратора безопасности. Linux ЖТЯИ.00087-01 91 04. Руководство администратора безопасности. FreeBSD ЖТЯИ.00087-01 91 05. Руководство администратора безопасности. Solaris ЖТЯИ.00087-01 91 06. Руководство администратора безопасности. AIX ЖТЯИ.00087-01 91 07. Руководство администратора безопасности. Mac OS Старая редакция: «При формировании закрытого ключа в контейнер записывается дата истечения срока действия этого ключа, по истечении которого в зависимости от настроек групповой политики возможны различные варианты использования этого ключа. Значение «0» групповой политики не накладывает никаких ограничений на использование ключа;

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
9	Значение «1» групповой политики запрещает формирование ЭП и шифрование в контексте этого ключа (возможно расшифрованные ранее зашифрованных сообщений); Значение «2» групповой политики запрещает любые действия с закрытым ключом. Срок действия ключа берется из (в порядке уменьшения приоритета): – Расширения контейнера ключа; – Расширения сертификата ключа; – Даты создания ключа + 1 год 3 месяца. Для операционных систем группы Windows выставить необходимое значение групповой политики можно в Редакторе локальной групповой политики (Выполнить -> gpedit.msc), в разделе «Классические административные шаблоны (ADM)». Для ключей алгоритма ГОСТ Р 34.10-2001 необходимо изменить значение ключа реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Crypto-Pro\CSP\ControlKeyTimeValidity2001. Выставление значения «0» для ключей алгоритма ГОСТ Р 34.10-2001 не допускается. Для ключей алгоритма ГОСТ Р 34.10-2012 как для коротких (256 бит), так и для длинных (512 бит) необходимо изменить значение ключа реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Crypto-Pro\CSP\ ControlKeyTimeValidity2012. Настройка СКЗИ для остальных ОС осуществляется с помощью утилиты cpconfig с помощью команды cpconfig -policy -set ControlKeyTimeValidity2001(2012) -value <значение>. 🕮 При работе в режиме усиленного контроля использования ключей (режим обязателен к использованию, отключение может производиться только в целях тестирования) значение групповой политики контроля срока действия пользовательских ключей принимается равным «2». …» Новая редакция: «… При формировании закрытого ключа в контейнер записывается дата истечения срока действия этого ключа, по истечении которого в зависимости от значения параметра ControlKeyTimeValidity возможны различные варианты использования этого ключа.

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
9	Значение «0» параметра не накладывает никаких ограничений на использование ключа. Значение «1» параметра запрещает формирование ЭП и шифрование в контексте этого ключа (возможно расшифрованные ранее зашифрованных сообщений) (значение по умолчанию); Значение «2» параметра запрещает любые действия с закрытым ключом. Срок действия ключа берется из (в порядке уменьшения приоритета): – Расширения контейнера ключа; – Расширения сертификата ключа; – Даты создания ключа + 1 год 3 месяца. Изменение параметра ControlKeyTimeValidity Для операционных систем группы Windows необходимо изменить значение ключа реестра HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Crypto Pro\Cryptography\CurrentVersion\Parameters\ControlKeyTimeValidity (для 64-битных операционных систем), HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\Parameters\ControlKeyTimeValidity (для 32-битных операционных систем). Настройка СКЗИ для остальных ОС осуществляется с помощью утилиты cpconfig с помощью команды ./cpconfig -ini \config\parameters -add long ControlKeyTimeValidity <значение> 🕮 При работе в режиме усиленного контроля использования ключей (режим обязателен к использованию, отключение может производиться только в целях тестирования) значение параметра ControlKeyTimeValidity принимается равным «2». …» ЖТЯИ.00087-01 91 08. Руководство администратора безопасности. iOS Добавлено: «…При встраивании СКЗИ КриптоПро CSP в приложения iOS должен быть включён режим усиленного контроля использования ключей. Режим усиленного контроля использования ключей обеспечивает осуществление контроля срока действия долговременных ключей электронной подписи и ключевого обмена, контроля доверенности ключей проверки электронной подписи и контроля корректного использования программного датчика случайных чисел.

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
9	Для включения этого режима в конфигурационный файл config.ini в раздел [Parameters] необходимо добавить строку: StrengthenedKeyUsageControl = 1 Для обеспечения корректного функционирования провайдера в части выработки электронной подписи, а также работы с временными ключами (в частности, для работы в рамках TLS-соединения без аутентификации клиента) и генерации случайных данных необходимо произвести выработку долговременных ключей, предварительно проверив, что зарегистрирован хотя бы один датчик случайных чисел. Использование СКЗИ без включения режима усиленного контроля использования ключей разрешается исключительно в тестовых целях…»
10	В документе ЖТЯИ.00087-01 91 02. КриптоПро CSP. Руководство администратора безопасности уточнены команды для проверки отделенной подписи. Старая редакция: «…- cpverify -versign FileName [SignValue] Проверка подписи ГОСТ 34.11 2012 (256 бит) для файла с именем FileName. SignValue - значение подписи в виде байтовой строки. Если параметр SignValue не передан, то значение подписи будет взято из файла «FileName.sgn». Подпись проверяется на открытом ключе из специального сертификата для подписи кода компании «КРИПТО-ПРО»…» Новая редакция: «…- cpverify -file_verify имя_файла [значение_подписи] -timestamp дата Проверка подписи файла с именем «имя_файла». Параметр «значение_подписи» необходимо передавать в виде байтовой строки. Если параметр «значение_подписи» не указан, то значение подписи берется из файла имя_файла.sgn. Параметр «дата» указывает, когда подпись была сформирована, необходимо указывать в формате дд.мм.гггг. Данная команда проверяет подпись с прямой последовательностью полубайт, для проверки подписи с обратной последовательностью байт необходимо использовать команду versign с аналогичным набором параметров. Подпись проверяется на открытом ключе из специального сертификата для подписи кода компании «КРИПТО-ПРО»…»

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
11	Для блокирования сбора телеметрии на ОС Windows 10/Server 2016 при загрузке операционной системы до старта системных служб удаляются конфигурации службы диагностики (DiagTrack) и записи событий трассировки (AutoLogger-DiagTrack-Listener) при включенном усиленном контроле. Служба диагностики и сборщики данных удаляются из системы и более не могут быть запущены. В документ ЖТЯИ.00087-01 91 02. Руководство администратора безопасности. Windows добавлено: «Для отключения функций телеметрии на ОС Windows 10/Server 2016 необходимо выполнить следующие действия: 1. Проверить наличие и статус сервиса DiagTrack (Панель управления -> Система и безопасность -> Администрирование -> Службы). 2. Если сервис запущен, то остановить его. 3. Удалить запись регистрации сервиса DiagTrack из реестра (Пуск -> выполнить -> regedit, раздел HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services. Здесь необходимо найти и удалить папку DiagTrack). 4. Удалить подготовленные к отправке данные, которые сохраняются в четырех файлах с расширением *.rbs, хранящихся в директории *%ProgramData%\Microsoft\Diagnosis*. Имена файлов для production сборок ОС – event00.rbs, event01.rbs, event10.rbs и event11.rbs. Для insider сборок ОС имена могут отличаться, поэтому необходимо удалить все файлы с расширением *.rbs. При возникновении проблем с удалением данных файлов необходимо в свойствах на вкладке «Безопасность» разрешить полный доступ к файлу, а затем удалить. 5. Остановить автоматическую (AutoLogger) ETW сессию *AutoLogger-DiagTrack-Listener*, которую DiagTrack активирует в процессе своей остановки. 6. Удалить файл, в который автоматическая (AutoLogger) ETW сессия *AutoLogger-DiagTrack-Listener* сохраняла собранные данные. Путь к файлу хранится в реестровой записи *AutoLogger-DiagTrack-Listener* в значении *FileName*. Конфигурации автоматических (AutoLogger) ETW сессий находятся в ключе реестра *HKLM\SYSTEM\CurrentControlSet\Control\WMI\AutoLogger*. Конфигурация целевой сессии хранится в данном ключе под записью *AutoLogger-DiagTrack-Listener*. В настоящее время данные сохраняются в файл *%ProgramData%\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-DiagTrack-Listener.etl*. 7. Удалить запись регистрации конфигурации автоматической (AutoLogger) ETW сессии *AutoLogger-DiagTrack-Listener* из реестра Данные действия необходимо выполнять после каждого кумулятивного обновления, поскольку данные обновления являются по сути полной переустановкой ОС и удаленные сервисы восстанавливаются.
12	В документ ЖТЯИ.00087-01 96 01. КриптоПро CSP. Руководство программиста добавлено: «Совместно с дистрибутивом поставляются следующие пакеты, позволяющие интегрировать «КриптоПро CSP» версии 4.0 в приложения, использующие OpenSSL API (такие как Web-сервер ngnix): cprocsp-cpopenssl, cprocsp-cpopenssl-base, cprocsp-cpopenssl-devel, cprocsp-cpopenssl-gost. Подробнее об их установке и настройке можно узнать на портале техподдержки и форуме КриптоПро.»