

Средство криптографической защиты информации "Континент-АП"

Версия 3.7 (исполнения 5, 6)

Комментарии к релизу 3.7.6.70

Документ содержит описание новых возможностей изделия "Средство криптографической защиты информации "Континент-АП". Версия 3.7 (исполнения 5, 6)" RU.88338853.501430.007 01 (далее – СКЗИ "Континент-АП", абонентский пункт, АП) версии 3.7.6.70 по сравнению с версией 3.7.5.220, а также особенностей работы и ограничений применения, которые необходимо учитывать при эксплуатации АП.

Оглавление

1.	Размещение файлов на компакт-дисках.....	3
1.1.	Диск 1.....	3
1.2.	Диск 2.....	3
2.	Изменения и новые возможности	4
2.1.	Версия сборки 3.7.6.70.....	4
3.	Ограничения на поддержку аппаратных и программных средств.....	5
4.	Особенности работы и ограничения	6
4.1.	Общесистемные	6
4.2.	Абонентский пункт.....	6

1. Размещение файлов на компакт-дисках

1.1. Диск 1

Каталог	Содержимое
Дистрибутивы	
\TS\	Дистрибутивы СКЗИ "Континент-АП"
\TS\VersionInfo.txt	Файл сведений о версии программного обеспечения абонентского пункта
\Sable\v.3.0	Программное обеспечение для поддержки совместной работы абонентского пункта с ПАК "Соболь" 3.0
\Sable\v.3.1	Программное обеспечение для поддержки совместной работы абонентского пункта с ПАК "Соболь" 3.1
\Sable\v.3.2	Программное обеспечение для поддержки совместной работы абонентского пункта с ПАК "Соболь" 3.2
\third_party\	Стороннее программное обеспечение, необходимое для работы СКЗИ "Континент-АП"
\token_libs\	Драйверы для поддержки ключевых носителей JaCarta и ESMART
\Tools\csum-2012.exe	Программа расчета контрольных сумм

1.2. Диск 2

Каталог	Содержимое
Документация	
\Эксплуатационная документация\ Continent-AP - Linux - Release Notes.pdf	Release Notes – сведения о новых возможностях, особенностях работы и ограничениях применения СКЗИ "Континент-АП"
\Эксплуатационная документация\ Continent-AP - Linux - Admin Guide.pdf	Документ "Средство криптографической защиты информации "Континент-АП". Версия 3.7 (исполнения 5, 6). Руководство администратора. Linux" RU.88338853.501430.007 01 91
\Эксплуатационная документация\ Continent-AP - Linux - User Guide.pdf	Документ "Средство криптографической защиты информации "Континент-АП". Версия 3.7 (исполнения 5, 6). Руководство пользователя. Linux" RU.88338853.501430.007 01 92
\Техническая документация\ RU.88338853.501430.007 01 93 - Правила пользования.pdf	Документ "Средство криптографической защиты информации "Континент-АП". Версия 3.7 (исполнения 5, 6). Правила пользования" RU.88338853.501430.007 01 93
\Техническая документация\ RU.88338853.501430.007 01 30 - Формуляр.pdf	Документ "Средство криптографической защиты информации "Континент-АП". Версия 3.7 (исполнения 5, 6). Формуляр" RU.88338853.501430.007 01 30
\Техническая документация\ Continent-AP - Linux - IC.pdf	Список файлов, устанавливаемых на контроль целостности при установке СКЗИ "Континент-АП"

2. Изменения и новые возможности

2.1. Версия сборки 3.7.6.70

- 1.** Реализована поддержка дополнительных ключевых устройств:
 - JaCarta PKI;
 - JaCarta-2 ГОСТ;
 - JaCarta ГОСТ;
 - JaCarta LT;
 - Рутокен Lite;
 - ESMART Token USB;
 - ESMART Token ГОСТ.
- 2.** Реализовано функционирование СКЗИ "Континент-АП" в среде следующих ОС:
 - Astra Linux Common Edition "Орел" 1.11, 2.11 x64;
 - Astra Linux Special Edition "Смоленск" 1.6 x64;
 - РЕД ОС 7.1 МУРОМ x64;
 - Альт Линукс СПТ 7.0.5 x86/x64;
 - Альт 8 СП x86/x64;
 - GosLinux 6.4 x86/x64 (ic2);
 - ROSA Enterprise Desktop X3 x86/x64.
- 3.** Добавлена защита PIN-кодом контейнеров закрытых ключей на поддерживаемых токенах (JaCarta, ESMART, Рутокен).
- 4.** Добавлено затирание пароля ключевого контейнера и PIN-кода ключевого носителя в клиенте после соединения.
- 5.** Реализована поддержка доменных пользователей.

3. Ограничения на поддержку аппаратных и программных средств

1	Ключевые устройства	АП	<ul style="list-style-type: none"> • USB-флеш-накопитель; • JaCarta PKI; • JaCarta-2 ГОСТ; • JaCarta ГОСТ; • JaCarta LT; • Рутокен ЭЦП 2.0; • Рутокен S (с драйвером от производителя); • Рутокен Lite; • iButton DS1994-DS1996 (при наличии ПАК "Соболь" 3.0/3.1/3.2); • ESMART Token USB; • ESMART Token ГОСТ
2	Операционная система	АП	<ul style="list-style-type: none"> • Astra Linux Common Edition "Орел" 1.9, 1.11, 2.11 x64; • Astra Linux Special Edition "Смоленск" 1.5, 1.6 x64; • CentOS 6.5 x86/x64; • ContinentOS 4.2 x64; • Debian 7.6 wheezy x86/x64; • RHEL 6.5 Desktop x86/x64; • RHEL 6.5 Server x86/x64; • RHEL 7.0 Desktop x64; • RHEL 7.0 Server x64; • GosLinux 6.4 x86/x64 (ic2); • РЕД ОС 7.1 МУРОМ x64; • Ubuntu 14.04 LTS Desktop x86/x64; • Ubuntu 14.04 LTS Server x86/x64; • Альт Линукс СПТ 7.0.5 x86/x64; • Альт 8 СП x86/x64; • ROSA Enterprise Desktop X3 x86/x64
3	Предыдущие версии СКЗИ "Континент-АП"	Обновление предыдущих версий	3.7.5.220
4	Устанавливаемые продукты	ПАК "Соболь" 3.0/3.1/3.2	Исполнение АП – 6

4. Особенности работы и ограничения

4.1. Общесистемные

1. Установку и удаление компонентов СКЗИ "Континент-АП" должен осуществлять пользователь, наделенный правами локального администратора данного компьютера.
2. Если в составе операционной системы установлена утилита prelink, это может привести к некорректной работе механизма контроля целостности. Для предотвращения некорректной работы необходимо перед установкой ПО АП удалить программный пакет с утилитой prelink или добавить все бинарные файлы из состава /etc/cts/filelist в "черный список" утилиты prelink. Для добавления файлов в "черный список" создайте в /etc/prelink.conf.d/ файл (например, cts-ext.conf) с содержанием вида `-b <binary_file>`.
3. В профиле подключения в настройках прокси-сервера при указании имени пользователя и пароля использование символов кириллицы запрещается.
4. Для корректной работы абонентского пункта при входе в систему доменным пользователем необходимо указывать полное имя домена.

4.2. Абонентский пункт

1. Для низкого уровня безопасности используется биологический датчик случайных чисел. Для среднего уровня используется ДСЧ ПАК "Соболь".
2. На компьютере с установленным СКЗИ "Континент-АП" не рекомендуется подключать одновременно два и более ключевых носителя одного типа с хранящимися на каждом из них закрытыми ключами. В противном случае соединение АП с сервером доступа не гарантируется.
3. Для поддержки работы Рутокен S требуются драйверы с официального сайта компании-разработчика (<http://www.rutoken.ru/>).

4. Импорт закрытого ключа поддерживается только с устройств:

- Рутокен S;
- Рутокен ЭЦП;
- iButton;
- USB-флеш-накопитель.

Импорт возможен только для ключей, зашифрованных паролем, состоящим из символов A – Z, a – z, 0 – 9.

5. Особенность использования ключевого носителя Рутокен S в среде ОС Astra Linux Special Edition "Смоленск" 1.6 x64, Astra Linux Common Edition "Орел" 2.11 x64, Альт Линукс СПТ 7.0.5 x86/x64, Альт 8 СП x86/x64, РЕД ОС 7.1 МУРОМ x64:

- Невозможно выполнить импорт закрытого ключа с носителя Рутокен S.
- Если закрытый ключ был создан в АП версии 3.7.5.220 и сохранен на носителе Рутокен S, то выполнить подключение в АП версии 3.7.6.70 с использованием этого закрытого ключа на Рутокен S в перечисленных ОС невозможно.

6. Особенность обновления абонентского пункта среднего уровня безопасности с версии 3.7.5 до версии 3.7.6. После обновления необходимо во всех профилях подключения с автоматическим подключением после входа пользователя в систему повторно указать пароль доступа к ключевому контейнеру.

Компания "Код Безопасности"

Почтовый адрес:	115127, Россия, Москва, а/я 66
Телефон:	8 495 982-30-20
Факс:	8 495 744-29-31
E-mail:	info@securitycode.ru
Сайт:	https://www.securitycode.ru