R301 ФОРОС USB, смарт-карта ФОРОС для Windows Руководство пользователя



ООО СмартПарк 2021

Оглавление

1	Общее описание	3
2	Перед применением	3
3	Вход в учетную запись Windows	4
4	Подпись и шифрования почты в Outlook	4
5	Цифровая подпись в Microsoft Office: Word, Excel, Power Point	8
6	Цифровая подпись в Adobe Reader	. 10
7	Шифрование данных EFS	. 12
8	Шифрование данных BitLocker	. 15

1 Общее описание

Носитель R301 ФОРОС USB/смарт-карта ФОРОС для Windows (далее - Форос-Windows) предназначен для применения в качестве персонального электронного идентификатора в ОС Windows (7, 8.1, 10) в рамках информационной технологии компании Microsoft.

Аутентификация при помощи Форос-Windows позволяет кардинально повысить безопасность системы, снижает риск несанкционированного доступа. Использование Форос-Windows позволяет внедрить двухфакторную аутентификацию в следующие сценарии использования:

- аутентификация при входе в ОС Windows (winlogon);

- аутентификация в VPN-соединениях;

- аутентификация при доступе к удаленному рабочему столу по протоколу RDP;

- аутентификация при доступе к интернет ресурсам.

Также Форос-Windows можно использовать для:

- защиты электронной почты в Microsoft Outlook;
- подписи документов Microsoft Office;
- подписи pdf документов;

- шифрования отдельных файлов и целиком разделов жестких дисков (EFS, BitLocker).

Форос-Windows обеспечивает неизвлекаемость ключевой информации из носителя. Неизвлекаемость означает, что ключ применяется исключительно внутри микроконтроллера Форос-Windows и не может попасть на жёсткий диск компьютера или в оперативную память. При этом для применения Форос-Windows требуется знание ПИН-кода пользователя. Для защиты от подбора значения ПИН-кода присутствует механизм блокировки ПИН-кода. При 5 неверных попытках подряд ввести ПИН-код он заблокируется.

Для всех применений Форос-Windows, кроме шифрования EFS, требуется, чтобы компьютер, на котором применяется Форос-Windows, был членом домена. Соответственно должен быть сервер являющийся контроллером домена и сервер являющийся центром сертификации.

2 Перед применением

Процедура установки драйверов Форос-Windows описана в Руководстве администратора (раздел 2).

Перед непосредственным применением пользователем Форос-Windows

его необходимо персонализировать, то есть записать ключ и сертификат. Данная процедура описана в Руководстве администратора.

Для обеспечения безопасности пользователь должен сменить транспортное значение ПИН пользователя Форос-Windows на рабочее. Для либо этого надо использовать административную утилиту UnblockForosWindows (её описание приведено в Руководстве администратора), либо это можно выполнить средствами Windows после установки драйверов Φopoc-Windows. Для этого необходимо подключить Форос-Windows к компьютеру, нажать сочетание клавиш Ctrl+Alt+Delete и выбрать опцию «Изменить пароль». После чего будет предложено ввести старый и новый ПИНкод. Минимальная длина ПИН-кода 4 символа, максимальная – 8 символов. ПИН-код может состоять из любых печатных символов.

Транспортное значение ПИН-код Пользователя, устанавливаемое производителем Форос-Windows: «11111111».

3 Вход в учетную запись Windows

Форос-Windows обеспечивает двухфакторную аутентификацию при входе в учетную запись Windows (физическое наличие носителя у Пользователя и знание Пользователем ПИН-кода пользователя). Для этого персонализированный Форос-Windows подключите к компьютеру, состоящему в том же домене, что и центр сертификации. Загрузите ОС. Выберите «Параметры входа» («Sign-in options») и затем выберите иконку смарт-карты.

ОС считает данные с Форос-Windows и выведет на экран имя пользователя. Введите ПИН-код.

При следующем входе в ОС опция использования Форос-Windows будет активна по умолчанию.

Таким образом, для входа в учетную запись пользователя необходимо наличие Форос-Windows и знание ПИН-кода.

4 Подпись и шифрования почты в Outlook

Используя Форос-Windows, на который записан сертификат и ключевая пара, пользователь может защитить свою электронную почту – подписать и зашифровать электронное сообщение.

Цифровая подпись сообщений позволяет подтвердить:

- личность отправителя
- что содержимое сообщения не было изменено после подписания

Цифровая подпись почтовых сообщений производится отправителем сообщения с использованием своего закрытого ключа. Получатель сообщения

при помощи открытого ключа может проверить цифровую подпись. Открытый ключ передаётся внутри сертификата, который прикладывается к подписанному сообщению. С помощью сертификата получатель также посмотреть информацию об отправителе.

Зашифрование электронного сообщения производится на открытом ключе получателя. Получатель расшифровывает полученное сообщение на своём закрытом ключе. Поэтому прежде чем шифровать сообщение, получатель и отправитель должны обменяться открытыми ключами. Обмен открытыми ключами производится путём отправки сообщения с электронной подписью и сертификатом.

Описание применения Форос-Windows приведено на примере Outlook 2010. В других версиях действия аналогичные. Пункты 1-5 касаются настройки Outlook. Их можно доверить администратору. Непосредственно описание применения Форос-Windows для подписи и шифрования сообщений начинается с пункта 6.

1. Выберите Файл->Параметры. В отобразившемся окне, в левом меню выберите «Центр управления безопасностью» и справа нажмите «Параметры центра управления безопасностью».

0 🗄 🔊 📼		Входящие - soloviev@smart-p	oark.ru – Microsoft Outlook (I	Сбой активации про	дукта)		- 0 ×
Создать Новые сообщение элекенты Колдать Создать Новые Создать Создать Создать	авка и получение Папка Вид Пропустить Эчистка * Удалить Удалить Удалить Удалить	Ответить	Ререместить в: ? ∧	 Переместить * Правила * ОпеNote Переместить 	 Прочитано? Выбрать категорию * К исполнению * Теги 	Найти контакт • М Адресная книга Фильтр почты • Найти	© Отправить и получить почту - все папки Отправка и получение
Содать	Уданить С Г Параметры Outlook Общие Почта Календарь Контакты Задачи Заметки и дневник Поиск Мобильные Язык Дополнительно Настройка ленты Панель быстрого доступа Надстройки Центр управления безопасностью	Ответить Обеспечение безо Зацита конфиденциальност Корпорация Майкорсофт Мискозоft Unlook помогое <u>Показать заявление о ко</u> <u>Завяление о конфиденц</u> <u>Поговали улучшения к</u> <u>Везопасность и другие сведии</u> <u>Дополнительные сведения</u> <u>Создание защищению и</u> <u>Центр управления безопасто</u> <u>Центр управления безопасто и конфиден</u> <u>обеспечить безопасность и</u> рековнендуется.	Быстрые действия 15 16 17	Переместить аске безопасности щильности, чтобы и полость, см. заявление 1 Outlook	Теги и и работоспособности к получить дополнительные о конфиденциальности.	Найти ? × омпьютера. ведения о том, как	Отправка и получение И вт ср Чг Пл Сб Вс 29 30 31 1 2 3 4 5 6 7 8 9 10 1 12 13 14 15 16 17 8 19 20 21 22 23 24 5 26 27 28 29 30 31 1 2 3 4 5 6 7 еч в будущем не намечено.
Почта	Сергеев Дмитрий		18.12.2020	Remind	er - Deprecation of SHA-1	Chincina .	
 Календарь Контакты Задачи Задачи 		Форос 2 на сайт СмартПарка Форос 2 на сайт СмартПарка Форос 2 на сайт СмартПарка	18.12.2020 🛛 🏹 17.12.2020 🖓 🏹	Authent Timesta	amping - January 26th, 20		100%
элементы чч ттепрочитанн	a.c. 50						

2. В окне Центр управления безопасностью выберите «Защита

электронных писем». Если необходимо включить подпись ко всем письмам по умолчанию, то отметьте пункт «Добавлять цифровую подпись к исходящим сообщениям».

Центр управления безопасностью	? ×
Надежные издатели Параметры конфиденциальности	Шифрованная электронная почта
Защита электронной почты Обработка вложений Автоматическая загрузка	 Добавлять цифровую подпись к исходящим сообщениям Отправлять подписанные сообщения открытым текстом Запрашивать уведомление S/MIME для всех подписанных сообщений S/MIME По умолчанию: Защищенное сообщение
Параметры макросов Программный доступ	Цифровые удостоверения (сертификаты)
	Цифровые удостоверения или сертификаты являются документами, которые обеспечивают безопасность ваших электронных транзакций. Импорт/ <u>э</u> кспорт <u>П</u> олучить удостоверение
	Читать как обычный текст
	Читать обычные письма как обычный текст Читать письма с цифровой подписью как обычный текст
	Скрипты в папках
	☐ Разрешит <u>ь</u> скрипты в общих папках ☐ Р <u>а</u> зрешить скрипты в общих папках
	ОК Отмена

Нажмите «Параметры». 3.

В открывшемся окне выберите сертификат подписи и алгоритм 4. хэширования. Если планируется использовать шифрование, то выберите алгоритм шифрования.

Изменение настройки безоп	асности	×
Настройка безопасности Имя конфигурации:		
Защищенное сообщение		~
Формат криптографии:	S/MIME	\sim
Иастройка безопасности	по умолчанию для этого формата	
Иастройка по умолчаник	о для всех сообщений	
Метки безопасности	Создать Удалить	Пароль
Сертификаты и алгоритмы		
Сертификат подписи:	Соловьев Антон	Выбрать
Алгоритм хеширования:	SHA256 \checkmark	
Сертификат шифрования:	Соловьев Антон	Выбрать
Алгоритм шифрования:	AES (256-bit) \lor	
🗹 Передавать сертификат	ы с сообщением	
	ОК	Отмена

5. После нажатия на кнопку «Выбрать...» в открывшемся окне необходимо выбрать нужный сертификат. Нажмите ОК.

6. Создайте новое письмо. Заполните необходимые данные для отправки.

7. Выберите в верхнем меню «Параметры».

8. На открывшемся меню доступны две кнопки «Подписать» и «Шифровать». Если ранее был выбран пункт «Добавлять цифровую подпись к исходящим сообщениям», то кнопка «Подписать» уже будет активна. Соответственно на данном шаге можно включить/отключить подпись и шифрование сообщения.

9. Если настройки по умолчанию корректны и их менять не надо, то пункт 8 можно пропустить.

10. Убедитесь, что к компьютеру подключён Форос-Windows.

11. Нажмите кнопку «Отправить», появится окно ввода ПИН-кода. Введите ПИН-код и нажмите «ОК».



12. Подписанные письма будут отмечены специальным значком.

5 Цифровая подпись в Microsoft Office: Word, Excel, Power Point

К документам, созданным посредством программ Microsoft Office можно добавлять цифровую подпись.

Цифровая подпись электронных документов позволяет убедиться, что содержимое данных документов не было изменено после процедуры подписания.

Описанный ниже пример дан на основе Word 2010, в остальных продуктах и версиях Microsoft Office цифровая подпись делается аналогично.

1. Откройте необходимый документ Microsoft Word.

2. Выберете меню «Файл->Сведения->Защитить документ->Добавить цифровую подпись»

Файл Главная Вставка	Разметка страницы Ссылки Рассылки Рецензирование Вид		
🚽 Сохранить 🔣 Сохранить как 🚰 Открыть	Сведения: Документ2		
🍯 Закрыть	Містозоft Office профессиональный плюс 2010 требует действительной		
Сведения	лицензии для продукта. Чтобы получить действительную лицензию для продукта активируйте ключ продукта сейчас.		
Последние		Can Marana a	
Создать Печать	Разрешения Все могут открывать, копировать и изменять любую часть этого документа.	Своиства * Размер Число страниц Число слов Общее время правки	Еще не сохранен 1 0 0 мин
Сохранить и отправить	Пометка документа как окончательный Пометка документа как окончательного и нередактируемого.	Название Теги Примечания	Добавить заголовок Добавить тег Добавить примечания
🗈 Параметры	Зашифровать паролем му файлу необходимо Требует пароль для открытия данного документа.	Связанные даты	Никогла
🔀 Выход	Ограничить редактирование	Создан	Сегодня, 11:39
	Управление типами изменений, которые разрешено вносить пользователям в этот документ.	Напечатан	Никогда
	Ограничить разрешения для пользователей	Связанные пользовате	ели
	возможности изменения, копирования и печати.	Автор	Антон Соловьев
	Добавить цифровую подпись Обеспечение целостности документа путем добавления	Кем изменено	Еще не сохранен
	กรรมนูทสงท แหลูมุขรอง กอนุกสงร.	Показать все свойства	

3. Появится окно «Подписание». С помощью кнопки «Изменить» можно выбрать сертификат, используемый для подписи документа.

Подписание			?	×
Дополнительные	е сведения о том, что подписые	зается		
В документ будет доб просмотре содержимо	авлена цифровая подпись. Эта го документа.	подпись не буде	ет видна при	1
Цель подписания доку	умента:			
Тема сертификата: Кем выдан:	Соловьев Антон SMARTPARK-TEAM2012-CA		Изменит	ъ
		Подписат	ь Отм	ена

4. Появится окно ввода ПИН-кода. Введите ПИН-код и нажмите «ОК».

5. В документе будет отображена информация, что он подписан и является окончательным. Можно посмотреть, кто подписал документ, сертификат подписавшего. Для этого необходимо выбрать «Файл->Сведения->Просмотр подписей» или кликнуть на иконку подписи внизу документа.

Руководство пользователя

Φopoc-Windows



6 Цифровая подпись в Adobe Reader

К документам, созданным посредством программ Adobe Acrobat или Adobe Reader можно добавлять цифровую подпись.

Подпись на основе сертификата, как и обычная подпись шариковой ручкой, идентифицирует лицо, подписавшее документ. В отличие от рукописной, такую подпись очень сложно подделать, так как она содержит зашифрованную, уникальную для подписывающего информацию. Получатели документа могут легко проверить подпись, а также определить, был ли документ изменен после того, как был подписан.

Описанный ниже пример дан на основе Adobe Acrobat Reader DC.

- 1. Откройте pdf документ, который необходимо подписать.
- 2. Выберите «Инструменты->Сертификаты».
- 3. Выберите меню «Поставить цифровую подпись»

Φopoc-Windows



4. Выделите область в подписываемом документе, где будет отображаться подпись.



Нажмите

5. Выберете необходимый сертификат для подписи. «Продолжить»



6. Настройте оформление подписи и завершите процесс подписи, введите ПИН-код.

7 Шифрование данных EFS

В Windows существует встроенная технология шифрования данных EFS. Эта технология позволяет шифровать каждый файл по отдельности. Помимо этого особенностью данной технологии является локальная работа, то есть пользователь сам создает ключ на Форос-Windows и никак не привязан к домену.

Данные, зашифрованные с помощью EFS, могут быть расшифрованы только с помощью той же самой учётной записи Windows, из-под которой было выполнено шифрование. Также для расшифровки будет необходимо подключить к компьютеру Форос-Windows и ввести ПИН-код.

1. Сначала необходимо выпустить и записать сертификат и закрытый ключ в Форос-Windows. Выберите «Пуск->Панель управления->Учетные записи пользователя». В открывшемся окне выберите «Управление сертификатами шифрования файлов».

Руководство пользователя

🎎 Учетные записи пользователей		- (×
$\leftarrow \ ightarrow \ \uparrow \ \& \ll$ Все элемент	ты панели уп > Учетные записи пользователей 🛛 🗸 🗗 Поиск в па	нели управле	ения	9
Файл Правка Вид Сервис		${\bf x} \checkmark$		۲
Панель управления — домашняя страница	Параметры папок Внесение изменений в учетную запись пользователя			?
Администрирование учетных записей Управление сертификатами шифрования файлов	Изменение учетной записи в окне "Параметры компьютера"	Антон Со SMART\solo	ЛОВЬ6 viev	ев
Управление профилями пользователей	Изменить параметры контроля учетных записей			
Изменение переменных среды	Управление учетными записями пользователей Чтобы изменить пароль, нажмите клавиши CTRL+ALT+DELETE и выберите	"Сменить пар	роль".	

Форос-Windows

2. Если в Форос-Windows уже есть сертификат, то для дальнейшей работы можно использовать его. Необходимо нажать «Выбрать сертификат» и выбрать соответствующий. Можно создать новый сертификат на Форос-Windows. Для этого необходимо выбирать «Создать новый сертификат» и нажать «Далее». В окне «Создать сертификат» выберите самозаверяемый сертификат с сохранением его на смарт-карте и нажмите «Далее».

	\times	
🔶 🛛 Шифрующая файловая система (EFS)		
Создать сертификат		
О Создать новый самозаверяющий сертификат и сохранить его на моем компьютере		
Создать сертификат, чтобы защитить файлы в случае потери компьютера		
Создать новый самозаверяющий сертификат и сохранить его на моей смарт-карте		
Создайте сертификат, чтобы защитить файлы в случае потери компьютера. При доступе к файлам, зашифрованным с помощью этого сертификата, необходимо использовать смарт-карту. Вставьте смарт-карту, если применяется этот вариант.		
Получить сертификат, выданный центром сертификации моего домена Сертификат этого типа использует параметры шифрования, выбранные системным администратором. Подключитесь к домену и в случае использования смарт-карты вставьте ее.		
Далее Отмен	a	

3. Введите ПИН-код смарт-карты.

4. В дальнейших окнах можно обновить ранее зашифрованные файлы, данную опцию в примере пропускаем.

Φopoc-Windows

5. Далее необходимо указать файл или директорию, которая будет зашифрована со всем содержимым, можно зашифровать весь диск со всеми вложенными директориями. Щёлкните правой кнопкой по директории и выберите «Свойства». Затем нажмите «Другие».

Предыдуи	цие версии	Настройка
Общие	Доступ	Безопасност
L	chm	
Гип:	Папка с файлами	
Расположение:	D:\tmp\1\1	
Размер:	1,90 MБ (2 000 189 ба	йт)
На диске:	1,91 ME (2 011 136 da	йт)
Содержит:	Файлов: 7; папок: 0	
Создан:	30 января 2020 г., 12	:52:14
Атрибуты:	Только для чтения (применимо тольк)	а о к файлам в папке
	Скрытый	Другие

6. В открывшемся окне выберите «Шифровать содержимое для защиты данных» и нажмите «ОК».

Допол	нительные атрибуты	\times	
¥	Установите подходящие параметры для этой папки. При изменении этих параметров вас спросят, хотите ли ви применять изменения к вложенным папкам и файлам.	ы	
Атрибуты индексирования и архивации Папка готова для архивирования Разрешить индексировать содержиное файлов в этой папке в дополнение к свойствам файла			
Атри СС С	буты скатия и шифрования жинать содержиное для экононии места на диске Іифровать содержиное для защиты данных Подробно 		

7. Затем нажмите «Применить». В открывшемся окне выберите «К данной папке и ко всем вложенным папкам и файлам». И нажмите «ОК».

Подтверждение изменения атрибутов	×
Выбраны следующие изменения атрибутов:	
Вы хотите применить эти изменения только к этой папке или также ко	
всем вложенным папкам и файлам? О Применение изменений только к этой папке	
●К данной папке и ко всем вложенным папкам и файлам	
ОК Отмена	

8. Чтобы проверить корректную работу шифрования файлов, выйдете из системы и войдите без Форос-Windows. Перейдите в зашифрованную

директорию и попробуйте открыть какой-либо файл. Если все настройки сделаны верно, отобразится предложение вставить смарт карту.

8 Шифрование данных BitLocker

Во всех операционных системах Microsoft Windows существует встроенная технология шифрования разделов жёстких дисков — BitLocker. Данная технология предназначена для шифрования разделов жесткого диска целиком. Есть возможность зашифровать целиком внешний носитель.

Шифрование производится посредством алгоритма AES. Ключ шифрования можно безопасно хранить на Форос-Windows.

BitLocker в отличии от EFS-шифрования работает только в рамках домена. Требуется наличие сервера и локальная работа технологии невозможна.

1. Откройте Проводник. Выберите диск, который необходимо зашифровать.

2. Щёлкните правой кнопкой диск, в отобразившемся меню выберите «Включить BitLocker».



3. Отметьте «Использовать смарт-карту для снятия блокировки диска», нажмите «Далее».

		×
4	— 🎭 Шифрование диска BitLocker (G:)	
	Выберите способы разблокировки диска	
	🗌 Использовать пароль для снятия блокировки диска	
	Пароли должны содержать прописные и строчные буквы, цифры, пробелы и символы.	
	Введите свой пароль	
	Введите пароль еще раз	
	🗹 Использовать смарт-карту для снятия блокировки диска	
	Необходимо будет вставить смарт-карту. ПИН-код смарт-карты потребуется при снятии блокировки с диска.	
	Далее Отмен	ia

4. В появившемся окне выберите способ сохранить ключ восстановления, в файл или отправить на печать. Этот ключ можно будет использовать для разблокировки диска в случае утери Форос-Windows.

5. Следующим шагом укажите, какую часть диска требуется зашифровать. Шифровать только занятое место на диске или весь диск.

6. Нажмите «Начать шифрование».

7. Будет отображаться трока состояния шифрования диска.

8. Когда процесс шифрования завершиться, будет выведено соответствующее сообщение и появится кнопка «Закрыть».

9. Перезагрузите компьютер. После перезагрузки подключите Форос-Windows к компьютеру. Откройте проводник.

10. Около зашифрованного диска должен появится значок замка. Щёлкните на данный диск и выберите вариант разблокировки «смарт-карта». Введите ПИН-код.

11. Содержимое диска должно открыться, в значок диска должен измениться на открытый замок.