КриптоАРМ

презентация отправки и получения пакета документов подписанных электронной подписью



1. Выбор документов и отправка на подпись

Выбираем нужные файлы и правой кнопкой в контекстном меню нажимаем «КриптоАРМ» и «Подписать и зашифровать»

от компьютер > Загрузки > archive-28.09.2018 > Files for signing	
 КриптоАРМ Проверка с использованием Windows Defender Отправить Предоставить доступ к Добавить в архив Добавить в архив "Files for signing.rar" Добавить в архив и отправить по е-mail Добавить в архив "Files for signing rar" и отправить по е-mail 	 Подписать Добавить подпись Заверить подпись Зашифровать Подписать и зашифровать Проверить подпись Снять и проверить ЭП Расшифровать
Отправить Вырозать	Просмотреть документ Расшифровать и проверить подпись
Копировать	Проверка сертификата на квалифицированность Квалифицированная подпись Упроциенный ражим работы
Удалить Переименовать	Профили >
Свойства	

2. Мастер создания ЭП и шифрования файлов

Откроется мастер создания электронной подписи и шифрования файлов

Нажимаем «Далее» -«Далее» до окна выбора сертификата

КриптоАРМ :: Под	писать и зашифровать	nun Maaran	×			
65	Вас приветст создания электг шифрован Для выполения операции 1) файл с данными для по 2) сертификат открытого	вует мастер Вибор файлов Выберите файлы исхо	ть и зашифровать одных данных для п	Х КриптоАРМ :: Подписать	и зашифровать	×
D	формирования подписи, и закрытому ключу	Имя fruit collection.zip	Размер Д 8.9 MB 31	Параметры подписи Установите желаемые г	параметры подписи	69
0	 сертификаты получате данных 	lemon juice.doc orange juice.jpg sugar nougat.xlsx apple syrup.doc	286.5 KB 09 1.4 MB 26 7.8 KB 02 37.0 KB 22	Свойства подписи Использование подписи: Комментарий к подписи:	[Не задано]	~
"\)	Для упрощения работы в установленные параметр	cherry pie.pdf crimson tea.pdf	1.7 MB 19 5.0 MB 19	Идентификатор ресурса: Поместить имя исходно	Определяется программой ого файла в поле "Идентификатор рес	ypca*
1	Наименование: Новыи пр	Добавить файл	Добавить папку	Включить в подпись: Сохранить подпись в о Удалить исходны	Только сертификат владельца тдельном файле й файл после выполнения операции	~
	< <u>Н</u> азад		< <u>Н</u> азад	Уровень безопасного Включить время созда Включить штамп време Включить штамп време Включить в полико о	удаления: Выключено	
					< Назад Далее >	Отмена

3. Выбор сертификата подписи

В окне «Параметры подписи» нажимаем на кнопку «Выбрать»

В окне «Хранилище сертификатов» выбираем личный сертификат для подписи и нажимаем «Ок»

Вернувшись в окно «Параметры подписи» нажимаем «Далее»

	Хранилище сертификатов	– 🗆 X
ертификат для создания подписи Владелец сертификата:	Назначение: <Любое>	КриптоАРМ :: Подписать и зашифровать
Хеш алгоритм:	Личное хранилище сертификатов Владелец Фамилия	Параметры подписи Установите желаемые параметры подписи
< Наза	234 ≥ 543 ⇒ Fargo Steel ⇒ Minoly Fermi ⇒ Refo Misa ⇒ Курзенев Алекса Курзенев Але ⇒ 000 °ЦИФРОВЫЕ Курзенев ⇒ 000 °ЦИФРОВЫЕ Селедкин <	Сертификат для создания подписи Владелец сертификата: CN=Fargo Steel, O=Fargo Steel Ltd, L=Ankar Хеш алгорити: GOST R 34.11-94 Выбрать Просмотрет

4. Архивирование подписанных файлов

Опционально

Если подписываете сразу несколько файлов, то перед шифрованием рекомендуем их архивировать.

		PIC.				
ODE	R-кодировка	*.	enc			
• ВА	SE64-кодиров	ка *.	enc			
	Отключить с	лужебные	е заголовки			
• Ap	хивировать ф	айлы пере	ед шифрова	нием		
Иг	1я файла: C	Users\an	s (Downloads	Varchive-28.	09.20:	Выбрать
Опо	мещать выхо,	цные файл	пы в указан	ный катало	-	
C:\U	sers\ans\Down	loads\arch	ive-28.09.20)18∖Files for	signing	Выбрать
	хранять стру	стуру вло:	женности ка	талогов		
		дные фай ю почтово	илы по элект ого клиента	гронной поч	те	

5. Шифрование в адрес получателей

В окне «Свойства шифрования» выберите тип криптопровайдера

Затем выберите сертификаты получателей, в чей адрес будет зашифрован пакет документов

КриптоАРМ :: Подписать и зашифровать Свойства шифрования Выберите необходимые свойства шифрования		КриптоАРМ :: Подписать и зашифровать Выберите сертификаты получателей			×
Выберите необходимь	е свойства шифрования	Сертификаты по	лучателей:		🥹 КриптоАРМ :: Подписать и зашифровать 🛛 🗙
Режим шифрования для	отправителя сообщения	Владелец	Издатель	Действит	Выберите сертификаты получателей
Тип криптопровайд	🥝 Хранилище сертиф	рикатов	<u></u>		Сертификаты получателей:
Алгоритм шифрова	Назначение: <Любое>			 Настрои 	Владелец Издатель Действителен с Действителе
ОИспользовать собст Сертификаты д	Сертификаты друг Л	их пользователей Сертификаты из LDAP ичное хранилище сертификатов		аты из LDAP	
Бладелец сертифик Алгоритм шифрован Бладелец 543 Fargo Stee	Владелец 543 Fargo Steel	Фамилия	Имя От	ИНН	
Включить серти	₩inoly Fermi Курзенев Алекса Ю ООО "ЦИФРОВЫЕ ООО "ЦИФРОВЫЕ	. Курзенев Алексан . Курзенев . Селедкин	д Алекса Андрей	001215 001215	Добавить Удалить Удалить все Просмотр
	<				< Назад Далее > Отмена
	Обновить	росмотр Импо	рт Устан	ювить фильтр	3
	Добавить и продолжит	гь	ОК	Отмена	a

6. Результат выполнения операций

В последнем окне указаны все параметры операции. Нажимаем на кнопку «Готово», чтобы начать их выполнение.

Результат операции показывается в отдельном окне.

Статус «Успех» свидетельствует об успешном завершении операции

	Статус					
	Данные, необход шифрования, соб Параметры	димые дл Браны	пя электронной подп	исии		
200	Сертификат по Формат подпис Криптопровайд Формат шифрое Получатель 1 Входной файл 1 Входной файл 3 Ходной файл 3	дписи и цер зания 1 2 3	Fargo Steel BASE64-кодировка Crypto-Pro GOST R BASE64-кодировка Minoly Fermi C: \Users\ans\Downl C: \Users\ans\Downl C: \Users\ans\Downl	(* 34. (* 0at 0at >		
	Сохранить да использовани	інные <mark>в</mark> г я	профиль для дальней	ішего	2	
	Наименование:	Новый	профиль	\sim		
1	Настроить отобр в меню приложен	ажение ния "Упр	шагов Мастера Вы мо авление профилями".	жете	×	





7. Отправка архива с документами по e-mail

Полученный в результате архив зашифрован

Поэтому его абсолютно безопасно можно передать получателю по электронной почте

Только владелец закрытого ключа сертификата шифрования может расшифровать файл



8. Получение пакета и дальнейшие действия

от компьютер > Загрузки > archive-28.09.2018 > Files for signing > Принимающая сторона

Принимающая сторона сохраняет у себя файл с архивом.

 \checkmark

Выбирает архив правой кнопкой и нажимает «КриптоАРМ», «Расшифровать и проверить подпись».

Шифров	(Открыть				
23,9 IVID	0	КриптоАРМ	>	Подписать		
	⊕ (Проверка с использованием Windows Defender Отправить		Добавить подпись Заверить подпись		
-		Открыть с помощью	>	, Зашифровать		
	ا ب 🌉	Предоставить доступ к Добавить в архив	> -	Проверить подпись		
		Добавить в архив "архив.zip.rar" Добавить в архив и отправить по e-mail		Расшифровать		
	1 1	Добавить в архив "архив.zip.rar" и отправить по e-mail Восстановить прежнюю версию		Просмотреть документ Расшифровать и проверить подпись		
	(Отправить	>	Проверка сертификата на квалифицированность		
	Вырезать Копировать		Квалифицированная подпись Упрощенный режим работы Профили			
	1	Создать ярлык Удалить	Ī			
		Переименовать	_			

9. Расшифрование полученных файлов

Откроется мастер расшифрования и проверки подписи

Нажимаем «Далее» -«Далее» и «Готово»

Сертификат расшифрования можно не указывать, так как он находится автоматически

ание и проверка подписи	×	Стати	- 22
приветствует Мастер расш ных и проверки электронно	ифрования эй подписи!	Статус Данные для расшифрования и проверки корректности электронной подписи собраны	
🙆 КриптоАРМ :: Расшиф	оование и проверка	подписи	
		Сертификат расшифрования Minoly Fer	n 🔺
л Выбор файлов в Выберите файлы шиф расшифровать	рованных данных, ко	Разархивирование Включенс Включенс Включенс Включенс Включенс Включенс Разархивирование Включенс В	IC
и Имя архив.zip.enc	Размер Да 23.9 МВ 19	Сертификат расшифрования На данном шаге предоставляется возможность выбрать предпочтительный сертификат расшифрования и режим сохранения расшифрованных файлов Сертификат расшифрования Владелец сертификата: CN=Minoly Fermi, C=AU	ic ic n n Jero
		Выбрать Просмотреть Удалить ох	сете
Robanura daŭa	Reference many	Режим сохранения расшифрованных фаилов Каталог сохранения файлов:	
дооавить фаил	дооавить папку	Выбор О	гмена
	< <u>Н</u> азад	Сохранять структуру каталогов Снимать подпись Удалять файл подписи Уровень безопасного удаления файлов Выключено ~	
	ание и проверка подписи приветствует Мастер расшиных и проверки электронно бого криптоАРМ :: Расшифр Выбор файлов Выберите файлы шиф расшифровать Имя архив.zip.enc Добавить файл	ание и проверка подписи × приветствует Мастер расшифрования ных и проверки электронной подписи! КриптоАРМ :: Расшифрование и проверка п Выбор файлов Выберите файлы шифрованных данных, кот расшифровать Имя Размер Дат архив.zip.enc 23.9 МВ 19.1 Добавить файл Добавить палку	КриптоАРМ :: Расшифрования и проверка подписи Статус Данные для расшифрования и проверки подписи Выбор файлов Выбор файлов Выбор файлов Выбор файлов Выбор файлов Сертификат расшифрования и проверка подписи Сертификат расшифрования Мinoly Ferri Разархивирование Иня Размер Дат архив. zip.enc Добавить файл Добавить папку Сертификат расшифрования Сертификат расшифрования Сертификат расшифрования Выбрать Просмотреть Удалить Сертификат расшифрования файлов Каталог сохранения расшифрования файлов Каталог сохранения расшифрованных файлов Сертификат расшифрования расшифрования (Сертификата) Сертификат расшифрования Выбор Сертификата расшифрования Выбрать Просмотреть Удалить Удалять файл подписи Удалять файлов Выключено V

10. Результат расшифрования

В последнем окне указаны все параметры операции. Нажимаем на кнопку «Готово», чтобы начать их выполнение.

Результат операции показывается в отдельном окне.

Статус «Успех» свидетельствует об успешном завершении операции



11. Результат проверки подписи

Для просмотра детальной информации о результате выполнения операции нажимаем на «Детали»

Нажмите на кнопку «Менеджер сообщения», чтобы открылось окно «Управление подписанными данными»

Vcnex				Закрыть
Общее время операции:	00:00:14			<< <u>Де</u> тал
Закрыть окно, если н	нет ошибок и з	амечаний		
Вид операции	Время	Входн <mark>ой фа</mark>	йл:	Выходно
Расшифрование	00:00:02.70	C:\Users\ans	Download	C:\Users\
Разархивирование	00:00:00.35	C:\Users\ans	Download	apple syru
Опроверка подписи	00:00:01.69	C:\Users\ans	Download	
Проверка подписи	00:00:01.47	C:\Users\ans	Download	
?		a 100 - 1	18 1 1	3
			Менеджер	сообщения
Статус завершения опе Длительность выполне Входной файл: Выходной файл:	рации: ния операции:	Успех. 0:00:01.47 С:\Users\ans\E <не был созда	ownloads\arch ан>	nive-28.09.2

Franking and House						
Выбранный файл						
Подписанный документ:	C:\Users\an	s\Downloads\arch	ive-28.09.	2018\Fil	es for si	gnin
Файл подписи:						
Неподписанный документ	r:					
Имя документа:	cherry pie.p	df				
		Просмотр	реть	Cox	ранить	
Дерево подписей						
Статус Владе	Фамилия	Им	я Отчес	тво		
Fargo Steel	in.					Fa
✓ Fargo Steel						F
Fargo Steel						F. > 59
✓ Fargo Steel <	Добавить	Завери	пь	Прос	мотреть	F: > 50
Fargo Steel Тодпись: Операции	Добавить	Завери	Тъ	Прос	мотреть	F:
✓ Fargo Steel Колородиись: Операции Отправить подписанный	Добавить документ по е	Завери mail	пь	Прос	мотреть	F. 、 分 。
Содпись:ОперацииОперацииОперацииОперацииОперацииОперацииОперацииОперацииОперации	Добавить документ по е информацию о	Завери mail подписи	пь	Отп	мотреть равить ечатать	F.

Ø

12. Целостность документа и статус сертификата

Нажмите на нижнюю кнопку «Просмотреть», чтобы открыть информацию целостности электронной подписи, статусе сертификата и о построенной цепочке доверия до корневого сертификата.

Информация о подписи и серти	ификате	×			
Подпись Сертификат Статус	сертификата	Информация о подпис	си и сертификате	×	
Комментарий: Использование подписи: Комментарий: Идентификатор ресурса: Время создания: Алгоритмы Алгоритм подписи:	 file:cherry pie.pdf 19.10.2018 16:51: FOCT P 34.10-2003	Подпись Сертификат Сертификат де Серийный номер: Владелец Идентификатор (СМ Организация Город Страна Издатель	Статус сертификата ействителен. 12 00 2b 68 95 ее 00 9c 34 4d 66 9c Fargo Steel Fargo Steel Ltd Ankara TR	Информация о подписи и сертификате Подпись Сертификат Статус сертификата На данной странице отображен общий статус проверки сертификации. Щепочка действительна. Статус СТАТУС СТАТУС СТАТУС СТАТУС СТАТУС СТАТУС СТАТУС	полного пути
Алгоритм хеширования;	FOCT P 34.11-94	Идентификатор (CN) Организация Город) CRYPTO-PRO Test Center CRYPTO-PRO LLC Moscow	n	росмотреть
		Страна Срок действия сертиф Действителен с 01	RU риката 08.2018 10:15:00 до 01.11.2	Владелец: Fargo Steel Статус сертификата: Сертификат действителен Подробности статуса: Сертификат действителен	
	O	Срок действия закры: Действителен с	того ключа <отсутствует> до <отс	По локальному CRL v	Проверить
			ОК		

13. Протокол проверки электронной подписи

2

🚫 Подтверждена

🚫 Подтверждена

Протокол проверки электронной подписи создается каждый раз при проверке подписанных документов.

Создается в PDF формате и может быть подписан ЭП

Включается в вкладке «Общие» профиля



cherry pie.pdf.sig

19.10.2018 17:38:54 UTC+03

crimson tea.pdf.sig

2.3 Mb

6.8 M5

Fargo Steel, Fargo Steel Ltd

Fargo Steel, Fargo Steel Ltd

CRYPTO-PRO Test Center 2, CRYPTO-PRO LLC

CRYPTO-PRO Test Center 2, CRYPTO-PRO LLC

01.08.2018 10:15:00 - 01.11.2018 10:25:00 UTC+03