Формирование ЭП с помощью программы «КриптоАРМ»

С помощью программы "КриптоАРМ" вы можете подписать

• отдельный файл

• папку файлов (при этом будет создана подпись для каждого файла, входящего в указанную папку. Подписанные файлы автоматически сохраняются в папку с исходными данными)

Подписать данные (создать первичную электронную подпись) вы можете через:

- Главное окно программы
- КриптоАРМ Агент
- контекстное меню

Чтобы открыть главное окно программы "КриптоАРМ" активизируйте приложение "КриптоАРМ" (Пуск -> Программы -> Digt -> КриптоАРМ –> КриптоАРМ)

Для того чтобы подписать данные, выберите пункт меню Подпись...:

• Главное окно, вид "Пользователь":

Подпись и проверка подписи

🧿 Вернуться на главную страницу	
Подписат ала	🚁 Проверить подпись
🕢 Добавить подпись	😤 Снять и проверить подпись
🙀 Заверить подпись	🔐 Расшифровать и проверить подпись
🔮 Подписать и зашифровать	🔗 Просмотреть документ

Рекомендуется использовать наиболее удобный способ, позволяющий производить операцию подписи путем вызова правой клавишей мыши контекстного меню файла в проводнике Windows.

🖳 Концепция разви	ітия УЦ в Чувашской Республика	е без сокр.doc	190 KB	Документ М
💾 Концепция разви	пция развития УЦ в Чувашской Республике.doc		181 KB	Документ М
Формирование е,	Открыть Изменить Созд <u>а</u> ть Печать	энства респу	47 KB	Документ М
	🚳 КриптоАРМ 🛛 🔹 🕨	Подписать		
	К Проверить на <u>в</u> ирусы № Копирован <u>и</u> е NetWare	Добавить под Заверить под Зашифровать	цпись пись	
	Open With WinRAR WinRAR WinZip	Подписать и з	зашифровать дпись зрить ЭЦП	
	Send To	Расшифроват Просмотреть	ь документ	
	Cu <u>t</u>	Расшифроват	ь и проверить под	пись,,,
	<u>C</u> opy Create <u>S</u> hortcut Delete Rename	 Интерактивни Настройки 	ый режим работы	•
	P <u>r</u> operties			

Далее следуйте рекомендациям Помощника по выполнению операции:

На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек для подписи. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**.

КриптоАРМ :: Создание ЭЦП 🛛 🔀				
	Вас приветствует Мастер создания электронной цифровой подписи!			
	Для создания подписи вам необходимо выбрать:			
	1) файл с данными для подписи			
	 режим создания подписи: отделенная подпись или совмещенная с исходными данными из файла 			
	 дополнительные параметры подписи - время создания, идентификатор ресурса и ваш комментарий 			
	 сертификат открытого ключа для формирования подписи. Сертификат должен быть связан с ключевым контейнером, к которому вы имеете доступ 			
	Для упрощения работы вы можете выбрать уже установленные настройки параметров подписи:			
	Наименование:			
/	🔲 Использовать настройку по умолчанию			
	< Back Next > Cancel			

Выберите папку с файлами или отдельный файл, которые необходимо подписать (кнопки Добавить папку и Добавить файл соответственно).

КриптоА	РМ :: Создание ЭЦП				×
Выбо Ві	р файлов ыберите файлы исход	(ных данных для	создания подпис	и 🄇	B
Имя		Размер	Лата изменения		
Конц	цепция развития У	180.5 KB	22.11.2005 12:47	:28 C:'	\Dc
			-		-
•				1	
	Добавить файл	Добавить папк	у Эдалить	9далить в	ce
				_	
		< <u>B</u> ac	k <u>N</u> ext>	Canc	el

В открывшемся окне укажите кодировку и расширение выходного файла и требуется ли заархивировать подписанные файлы.

Выходной файл может быть сформирован в формате *.sig, *.p7s

Для формата PKCS#7 Message в Base64-кодировке вы можете указать флаг **Отключить** служебные заголовки (в этом случае в файле подписи не будут использоваться заголовки, указывающие начало и окончание блока с подписанными данными. Заголовки необходимы для того, чтобы можно было выполнять проверку ЭП <u>более ранними версиями</u> программы "КриптоАРМ").

оиптоАР	РМ :: Создание ЭЦП			×
Выхо , Вы	дной формат ыберите желаемый выход	цной формат файл	а подписи	3
Кодир	овка и расширение			
۲	DER-кодировка [×] .	sig		
0	ВАЅЕ64-кодировка ×.	sig		
	🔲 Отключить служебны	е заголовки		
	Архивировать файлы пос	ле создания подп	иси	
	Имя архива: С:\Docume	nts and Settings\info	o4\My Docu	Выбрать
		< <u>B</u> ack	<u>N</u> ext >	Cancel
			Trew >	Cancer

КриптоАРМ :: Создание ЭЦП 🛛 🔀			
Параметры подписи Установите желаемые параметры подписи			
Свойства подписи			
Комментарий к подписи:			
Идентификатор ресурса: Концепция развития УЦ в Чувашской Республи			
🔽 Поместить имя исходного файла в поле "Идентификатор ресурса"			
🔽 Сохранить подпись в отдельном файле			
🔲 Удалить исходный файл после выполнения операции			
🔽 Включить время создания подписи			
🔲 Включить штамп времени на подписываемые данные			
🔲 Включить штамп времени на подпись			
🗖 Включить в подпись доказательства подлинности			
< <u>B</u> ack <u>N</u> ext > Cancel			

Далее введите необходимые свойства подписи (комментарий к подписи*, идентификатор ресурса**, включение времени создания подписи).

* Комментарием к подписи может служить информация, предназначенная для прочтения людям, просматривающим подписанный документ (например, "Согласовано!")

** Под идентификатором ресурса понимается:

• путь до исходного, подписываемого файла (на компьютере или в Интернете, где находится данный файл)

• имя файла (указывается для того, чтобы в случае изменения имени файла получатель подписанного документа смог определить первоначальное его название)

Укажите необходимые параметры ЭП - личный сертификат для создания ЭП.

иптоАРМ :: Создание ЭЦП		×		
Выбор сертификата подписи Выберите сертификат подписи		() рогр нтер	амма «КриптоА нету, электрон	РМ» пре⊥ ной почт
Сертификат для создания подписи				
Владелец сертификата:				
Хеш алгоритм:	Хранилище сертификатов			_ 🗆
	Назначение: </td <td></td> <td>▼ +</td> <td>астроить</td>		▼ +	астроить
	Личное хранилище сертификат	тов	_	
Проверять сертификат в слу	Владелец Изда	тель	Лейств Лейс	тв
	Alexey I cryptopro t Test (Center CRYPTO	09.10.2 09.10	.2
	mail.cap.ru mail.c	ap.ru	10.02.2 11.02	.2
	mail.cap.ru mail.c	ap.ru	06.09.2 07.09 06.09.2 07.09	.2
	🧖 Алексей И. Ишалев САР г	root CA	11.05.2 10.05	.2
	🤍 Ишалев Алексей САЗС		27.11.2 27.11	.2
	Обновить Просмотр	Импорт	Установить	фильтр
		L	ок	Отмена
птоАРМ :: Создание ЭЦП			×	
Выбор сертификата подп	ИСИ			
Выберите сертификат под	іписи		I	
C				
сертификат для создания под	лиси М. И	0 - F		
Владелец сертификата: С	N=Ишалев Алексей Ивано	ВИЧ,U=I ОСКОМСВ	язь	
Хеш алгоритм: 🛛 🛛	OST R 34.11-94		•	
			_	
	Выбрат	ь Просмот	реть	
П проверять сертификать	s chymae a car			
	< <u>B</u> ack <u>N</u> ex	(t≻) Ca	ncel	

Для доступа к выбранному ключевому контейнеру введите пароль.

После сбора данных для создания ЭП возникнет окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был подписан файл.

КриптоАРМ :: Создание	эцп	X
	Статус Данные, необходимые для создания электронной подписи, собраны Параметры	
	Сертификат подписи Ишалев Алексей Иванови Формат подписи DER-кодировка (*.sig) Входной файл 1 C:\Documents and Settings Выходной файл C:\Documents and Settings • C:\Documents and Settings	
7	Наименование: info4 Настроить отображение шагов Мастера Вы можете в меню приложения "Управление настройками".	
	< <u>B</u> ack Finish Cancel	

Указанные параметры ЭП можно сохранить в настройку в качестве шаблона для дальнейшего использования. Для этого поставьте флаг в пункте **Сохранить данные в настройку для** дальнейшего использования и введите наименование настройки. Также вы можете сохранить все данные в уже существующую настройку, выбрав ее название из списка.

Начнется процесс подписи файла. Остановить процесс можно, нажав на кнопку Отмена.

Сформированный файл ЭП по умолчанию будет сохранен в тот же каталог, в котором находится файл с исходными данными. Имя файла ЭП совпадает с именем подписываемого файла, дополненным расширением (расширение соответствует выбранному выходному формату). Если файл с таким именем уже существует, сохраните его под другим именем, например:



После завершения операции возникнет окно **Результат выполнения операции**. Чтобы просмотреть детальную информацию о результатах создания подписи и используемых параметрах: имя исходного файла, имя выходного файла, статус завершения операции, длительность выполнения операции, нажмите кнопку **Детали** >>.

Если вы хотите просмотреть информацию об ЭП и сертификате подписчика, выделите запись в списке окна **Результат выполнения операции** и нажмите на кнопку **Менеджер сообщения**.

Результат выполно	ения операции (Создание электро	нно цифро 💶 🗅	<
Scnex 🕑			Закрыты	
🔲 Запустить масте	р снова		<< Детали	
🔲 Закрыть окно, е	сли нет ошибок и	замечаний		
Выполнение	Время	Входной файл:	Выходной фа	
Series 😳 Screek	00:00:02	C:\Documents and	Settin C:\Document	
Series 🕑 Screx	00:00:00	C:\Documents and	Settin C:\Document	:
1				
				1
		Me	неджер сообщения	
Статус завершения Длительность выпо Входной файл: Выходной файл:	операции: олнения операции	Ucnex. : 0:00:02. C:\Documents and Se C:\Documents and Se	ettings\info4\My Docum ettings\info4\My Docum	ľ

Откроется окно Управление подписанными данными, в котором вы можете просмотреть информацию о подписи и сертификате:

- просмотреть подписанный файл, нажав на кнопку Просмотреть напротив имени файла,
- сохранить по указанному пути, нажав на кнопку Сохранить,
- просмотреть информацию о подписи, сертификате и его статусе (кнопка Просмотреть)

🛞 Концепция разв	ития УЦ в Чувац	иской Республике без сокр	.d 💶 💴	
Исходные данные:	C:\Documents and	d Settings\info4\My Documents\;	ЭЦП\Концепі	
Открытые данные:	Концепция разви	тия УЦ в Чувашской Республи	ке без сокр.	
	·	Просмотреть С	охранить	
Дерево подписей-				
	ФИО Алексей Изранови	Организация	Подраздел	
	Инф	ормация о подписи и серт	ификате	×
	Π	одпись Сертификат Статус	сертификата	
	ĺ	🔏 Подпись действительна	3	
	۵,	Атрибуты подписи	0	
		Комментарий:	J	
		Идентификатор ресурса:	file:Концепция развити	я УЦ в Чувашс
Подписать	Заверить по,	Время создания:	19.10.2007 16:19:39	
	A	Алгоритмы		
		Алгоритм подписи:	GOST R 34.10-2001	
		Алгоритм хеширования:	GOST R 34.11-94	
📀 Руководство				
Адрес для контактов:	info@digt.ru			
			ОК	Cancel

Проверка электронной цифровой подписи

С помощью программы "КриптоАРМ" вы можете проверить корректность электронной цифровой подписи

• отдельного файла

• папки файлов (при этом будет проверена подпись каждого файла, входящего в указанную папку. Выходные файлы автоматически сохраняются в папку с исходными данными)

! Проверка корректности всех вариантов и типов подписи выполняется по единой схеме, за исключением следующего момента:

• При проверке совмещенной подписи сначала выполняется снятие подписи с данных и сохранение подписанных данных в отдельный файл, а после этого - собственно проверка корректности подписи. Поэтому для того чтобы проверить корректность совмещенной подписи, в контекстном меню программы выберите пункт Снять и проверить подпись.

• При проверке отделенной подписи выберите пункт Проверить подпись.

Проверить корректность электронной подписи вы можете через:

- Главное окно программы
- КриптоАРМ Агент
- контекстное меню

Для того чтобы проверить подпись к файлу:

1.На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек для создания подписи. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**.

2.



Выберите файл или папку файлов, подписанных ЭП, корректность которых необходимо проверить (кнопки Добавить папку и Добавить файл).

(риптоАРМ :: Проверка	подписи	×
Выбор файлов Выберите файлы подп	иси, которые желаете проверить	8
1/Mg	Размер Лата изменения	Путь
		CATE
Conver_1.xis.sig	19 KB 04.09.2006 12:17:46	CATE
Detuer 3 Ms sig	22 ND 04,09,2000 12;27;33	CATE
		>
Добавить файл	Добавить папку Удалить Уда	алить все
	< Назад Далее > 💦	Отмена

3.После сбора данных для снятия и проверки подписи возникнет окно с информацией о статусе операции и об используемых параметрах.

4.Если в файле подписи содержится одна подпись (нет дополнительных и/ или заверяющих), то проверяется корректность ЭП и действительность сертификата отправителя. Если в файле ЭП содержится более одной подписи, то проверяется корректность каждой подписи в коллекции.

Результат выполнения операции (Проверка ЭЦП)	
0 из 3 файлов обработаны	Отменить все
🗌 Запустить мастер снова	Детали >>
🔲 Закрыть окно, если нет ошибок и замечаний	

Откроется окно **Результат выполнения операции**, в котором отобразится статус операции. Если одна или несколько подписей не действительны, это будет отражено в статусе. Чтобы просмотреть детальную информацию о результатах проверки подписи и используемых параметрах: имя исходного файла, имя выходного файла, статус завершения операции, длительность выполнения операции, нажмите на кнопку **Детали** >>.

5. Если вы хотите просмотреть информацию о проверяемой ЭП и сертификате подписчика, выделите необходимую запись в списке окна **Результат выполнения операции** и нажмите на кнопку **Менеджер сообщения**.

Результат выпол	тне ния операци	ии (Проверка ЭЦП)				
Успех Закрыть						
🗌 Запустить маст	Запустить мастер снова					
🔄 Закрыть окно, е	🗌 Закрыть окно, если нет ошибок и замечаний					
Выполнение	Время	Входной файл	Выходной ф			
Subsection States State	00:00:01	C:\TEMP\ФОтчет_1.xls	C:\TEMP\ΦC			
S yonex	00:00:00	C:\TEMP\ФОтчет_2.xls	C:\TEMP\ΦC			
Series 🛇 Yonex	00:00:01	C:\TEMP\ФОтчет_3.xls	C:\TEMP\ΦC			
<			>			
		Менеджер	сообщения.			
Статус завершения операции: Успех. Длительность выполнения операции: 0:00:01. Входной файл: С:\TEMP\ФОтчет_1.xls.sig Выходной файл: <не был создан>						

Откроется окно Управление подписанными данными

🔕 ФОтчет_2.xls.sig - Управление подписанными дан 🖃 🗖 🔀				
Исходные данные:	C:\TEMP\ФОтчет_2.xl	s.sig		
Открытые данные:	ФОтчет_2.xls			
		Просмотреть)	Сохранить	
Дерево подписей-				
	ФИО	Организация	я Подраз	
Sve	tlana Rozhkova	Digt	Маркети	
🖃 🗌 💙 🛛 Sve	tlana Rozhkova	Digt	Маркети	
Sve	tlana Rozhkova	Digt	Маркети	
< 	Ш]		>	
Подписать	Заверить подпись	Просмотреть	Обновить	
	ОК	Отмена	Применить	

Вы можете просмотреть исходный файл и сохранить его по указанному пути (кнопки **Просмотреть** и **Сохранить** напротив поля **Открытые** данные).

Отчет о проверке подписи можно просмотреть, выбрав запись в поле Дерево подписей и нажав на кнопку **Просмотреть**. Откроется окно с информацией о подписи, сертификате и его статусе.

Закладка **Подпись** содержит информацию об атрибутах подписи, времени ее создания, используемых алгоритмах подписи и хеширования.

В закладке Сертификат вы можете просмотреть сведения о сертификате и проверить его статус. Также в этом окне доступна информация о владельце и издателе сертификата, сроках действия сертификата и возможных варинтах использования.

В закладке **Статус сертификата** отображен общий статус проверки полного пути сертификации. Вы можете проверить путь сертификации, выбрав способ проверки из выпадающего списка и нажав на кнопку **Проверить**

В закладке Штампы времени дается информация о штампе времени на подпись (для классической ЭП) и информация о штампах времени на подпись и доказательства подписи (для усовершенствованной ЭП)

Информация о подписи и сертификате 🛛 🛛 🔀				
Подпись	Сертификат Статус	сертификата Штампы времени		
Подпись действительна				
Атрибуты подписи				
Комментарий:		Комментарий		
Идентификатор ресурса:		file:ФОтчет_2.xls		
Время создания:		04.09.2006 12:06:55		
Алгоритмы				
Алгоритм подписи:		ГОСТ Р 34.10-2001		
Алгоритм хеширования:		ГОСТ Р 34.11-94		
		ОК 💦 Отмена		