Использование КриптоПро CSP в Outlook Express

Hастройка Outlook Express

Выберите пункт меню **Сервис, Учетные записи...** и нажмите на закладку **Почта**. В отображаемом списке учетных записей выберите ту, которую необходимо настроить, и нажмите кнопку **Свойства**. В отображаемом диалоге выберите закладку **Безопасность**.

Отображаемый диалог позволяет пользователю указать свои личные сертификаты, которые будут использоваться при выборе личных ключей пользователя для формирования электронной цифровой подписи и расшифрования входящих сообщений.

Как уже было отмечено раннее, в диалоге выбора сертификата отображаются только сертификаты, имеющие совпадающий адрес электронной почты и разрешенные для защиты электронной почты.

U6щие	Серверь	ы Подключение	Безопасность	Дополнительно
Сертиф Выбо цифр подп	рикат под ерите сер ровой код исывании	писи тификат подписи. , который будет и и сообщений с это	Тем самым вы : спользоваться п й учетной записі	зададите ри ыю.
<u>С</u> ерт	ификат:	test		Выбрать
Выб	ерите сер очаются в	тификат и алгори сообщения с циф	тм шифрования. Ровой подписью	Эти данные ос тем, чтобы
ими шиф Серт	могли во рованных ификат:	спользоваться по сообщений. test	лучатели при отг	правке вам В <u>ы</u> брать
ими шиф Серт Алго	могли во рованных ификат: фитм:	спользоваться по сообщений. test GOST 28147-89 (лучатели при отг 256-bit)	правке вам В <u>ы</u> брать

Выберите пункт меню Сервис, Параметры... и нажмите на закладку Безопасность.

Оощие	Чтение	Уведо	мления	Отправ	ка сообщений	Создание сообщения
Подписи Правописание		сание	Безопасность		Подключение	Обслуживание
ащита от ви Выби ((Ш Ш Ш Ш С С И С С И С С И С С И С С И С С И С С И С С И С	русов ерите зону безоп (зона <u>Интернет</u> э зона о <u>г</u> раниче редупреждать, ек е разрешать сохр ображения	асности для а (безопасі нных узлов сли прилож ранение илі	я обозревати ность ниже, (безопасною ения пытаю и открытие в	еля Internet E но возможні сть выше) гся отправит вложений, ко	xplorer: остей больше) ь почту от моего ин торые могут содер	иени. жать вирусы.
агружать из 🗹 Б езопасная г	ооражения локироват <u>ь</u> изоб ючта	ражения и ,	другое внеш	нее содержи	мое в сообщении в	а формате HTML.
Серт поль	ификат позволяе зователя при эле	я удостове эктронном (рять личнос обмене данн	ГЬ ІЫМИ.		Сведения
Для шиф	подписывания от рованных сообще	правляемь эний нужно	их сообщени иметь серти	й или получе фикат.	ния	учить сертификат)
	(ифровать содер) одписывать все ј	кимое и вл отправляем	ожения всех ные сообщен	исходящих ния	сообщений	Дополнительно

В отображаемом диалоге можно включить режимы Шифровать содержимое и вложения исходящих сообщений иВключить цифровую подпись во все отправляемые сообщения для того, чтобы шифрование и электронная цифровая подпись

выполнялись автоматически для каждого сообщения. Если эти режимы не включены, опции шифрования и подписи нужно будет включать для каждого отправляемого сообщения.

Нажмите кнопку Дополнительно. В отображаемом диалоге установите следующие режимы:

Шифровать при отправке шифрованной почты самому себе. Установка режима включения дает возможность отправителю расшифровывать отправленные им сообщения.

Добавлять мой сертификат при отправлении сообщений с подписью.

Установка этого режима автоматически будет добавлять сертификат отправителя ко всем сообщениям. Этот режим позволяет производить обмен сертификатами с использованием подписанного сообщения, а затем использовать полученные сертификаты для

последующего шифрования сообщений между адресатами.

Кодировать сообщения перед подписыванием (непрозрачная подпись). При включенном режиме сообщения и все вложения будут объединены в единое вложение с включенной в него цифровой подписью. Если режим выключен – подпись формируется в

виде одного отдельного вложения для всех вложений.

Автоматически добавлять сертификат отправителя в адресную книгу. При включенном режиме сертификаты, передаваемые в составе подписанного сообщения, будут автоматически добавляться в адресную книгу.

Дополн	ительные параметры безопасности 🛛 💽 🔀
Шифро	ванные сообщения
0	Предупреждать при стойкости шифрования сообщений меньше:
	168 бит
	🗹 Шифровать при отправке шифрованной почты самому себе
Сообще	ения с цифровой подписью
0	Добавлять мой сертификат при отправлении сообщений с подписью
-	Кодировать сообщения перед подписыванием (непрозрачная подпись)
	🗹 Автоматически добавлять сертификат отправителя в адресную книгу
Провер	ка отзыва сертификатов
	Проверять, не были ли отозваны сертификаты:
	О Іолько при нахождении в сети
	<u>Н</u> икогда не проверять
	ОК Отмена

Проверять, не были ли отозваны сертификаты:

только при нахождении в сети – установка флага проверки приводит к тому, что каждая операция формирования или проверки электронной цифровой подписи будет сопровождаться проверкой на отзыв сертификата.

Для проверки на отзыв используется **список отозванных сертификатов (CRL)**, информация о нахождении которого, записывается в виде дополнения в сертификате каждого пользователя. По умолчанию данная опция не включена, и Outlook Express

не отслеживает факта компрометации ключей пользователей.

никогда не проверять – проверка на отзыв не выполняется.

Отправка подписанных сообщений

Для создания и отправки подписанного сообщения нажмите кнопку **Создать сообщение** или выберите пункт меню**Файл, Создать, Сообщение**.

Выберите получателя сообщения (поле **Кому**) и введите тему сообщения. Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить**. Для отправки сообщения в подписанном виде проверьте состояние кнопки **Подписать**.

Она должна быть нажата и должен быть виден признак подписанного сообщения в правой части экрана.

Отправить	Ж Вырезать	Копировать	Вставить	У Отменить	Я Проверить	АВС Правописа	і) Вложить	Вах	
Кому:	mailtest@crypt	opro.ru							
Тема: Присоединить:	test								
	8		ккч∆	, E E Ø		3 = -	e. III		
						Правописа Вложить Важ			

После того, как сообщение подготовлено к отправке, нажмите кнопку **Отправить**. Если в ответ появится следующее предупреждение, то это означает, что сертификат был отозван.

Сертификат для данной учетной записи отозван.					
Программе Outlook Express не удалось найти дей сертификата на этом компьютере. Получить новы	ствующего ий сертификат?				
Да Отправить, не подписывая	Отмена				

Получение сертификата открытого ключа абонента для шифрования сообщений

Для шифрования сообщений в адрес других пользователей необходимо предварительно произвести обмен сертификатами. Для этого обычно достаточно переслать подписанное сообщение в адрес требуемого абонента (сообщение посылается вместе с

сертификатом отправителя). После получения сообщения и проверки электронной цифровой подписи производится автоматическое добавление адреса отправителя и его сертификата в адресную книгу.

Для контроля добавления выполните следующие действия. Откройте полученное подписанное письмо. Установите курсор на адрес отправителя и, нажав правую кнопку мыши, выберите пункт **Добавить в адресную книгу**.

🔿 test					
Файл Правка Вид	Сервис Сооб	щение Спр	вка		11
S	9 % Переслать		Х Удалить	() Предыду	»
От: лап Дата: 13 к Кому: mail Тема: test Безопасность: Под	Добавить в адр Найти Блокировать от Копировать	есную книгу правителя			8
test	Свойства				×
					1

Для того, чтобы проверить наличие сертификата абонента в адресной книге, нажмите на кнопку **Адреса** в основном меню и выберите запись с требуемым абонентом (см. Рисунок 2). Если в записи абонента отсутствует сертификат или сертификат не обновился

(у абонента был старый сертификат), удалите полностью запись абонента из адресной книги и получите от него подписанное сообщение еще раз. При этом должно произойти автоматическое создание записи с сертификатом.

划 Адресная книга - Ос	новное удо	стове рение			
файл Правка Вид Серви	ıс <u>С</u> правка				
Щт Ш Создать Свойства	× Удалить	В Поиск людей	Д Печать	🤹• Действие	
🛛 🔡 Общие контакты	Введите <u>и</u> ли	выберите из спи	иска:		
Ссновное удостовер	Имя 🗡	Электр	онная почта	Служебный тел	Домашни
	E mailtest	mailtest(Deryptopro.ru		
< >>	<		101		>
1 объекта(-ов)					



Отправка шифрованных сообщений

Для создания и отправки подписанного сообщения нажмите кнопку **Создать сообщение** или выберите пункт меню **Файл**, **Создать**, **Сообщение**.

Выберите получателя сообщения (поле **Кому**) и введите тему сообщения. Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить**.

Для отправки сообщения в зашифрованном виде проверьте состояние кнопки Зашифровать.

Она должна быть нажата и должен быть виден признак шифрованного сообщения в правой части экрана. После того, как сообщение подготовлено к отправке, нажмите кнопку **Отправить**.

При попытке зашифровать письмо на открытом ключе владельца отозванного сертификата, возникнет та же ситуация, что и при отправке сообщения, подписанного с помощью отозванного сертификата. А предупреждающее окно будет выглядеть так:



Проверка сертификата на отзыв

Периодичность издания списков отозванных сертификатов (СОС) определяется Удостоверяющим центром. Центр Сертификации издает СОС и публикует его в сетевом справочнике (при его наличии).

Пользователи должны регулярно обновлять СОС, хранящийся в локальном справочнике сертификатов, с использованием доступных средств.

Для контроля проверки сертификатов на отзыв выполните следующие действия.

Откройте полученное подписанное письмо. Нажмите кнопку – признак подписанного сообщения. Как уже было отмечено раннее, для автоматической проверки подписи на отзыв необходимо установить флаг **Проверять, не были ли отозваны сертификаты:**

только при нахождении в сети. В противном случае, в открывшемся диалоге в закладке **Безопасность** увидите следующее:

Общие Подробно	Безопасность	
Цифровая подпись	3	
Подписано:	mailtest@cryptopro.ru	
Содержимое не и:	зменено:	Дa
Подпись достовер	она:	Дa
Запрос безопасно	ого уведомления:	н/д
Проверка отзыва	сертификата:	Нет
Состояние отзыва:	Проверка отзыва сертификатов была отключена.	< >
Метка безопасности:		3. 3
Шифрование —		
Содержание и вло	жения зашифрованы:	Нет
Алгоритм шифров	ания:	Нет

При установленном флаге проверки, если сертификат не отозван, в графе Состояние отзыва получите Сертификат не был отозван, или не удалось получить информацию об отзыве этого сертификата.

Если же сертификат отозвали, то при открытии письма появится предупреждение: «Этот сертификат был отозван»

А при нажатии кнопки, в открывшемся окне во вкладке Безопасность будет значиться: Этот сертификат был отозван.