Использование КриптоПро CSP в Outlook 2002/2003

Особенностями использования почтовой программы Outlook 2002/2003 и сервера Exchange являются:

1. Криптопровайдер КриптоПро CSP поддерживает только формат S/MIME защищенных почтовых сообщений, и поэтому в настройках сервера Exchange должна стоять опция использования формата MIME и разрешения маршрутизации защищенных сообщений S/MIME.

2. Криптопровайдер КриптоПро CSP не поддерживает работу KMS сервера Exchange и хранения сертификатов открытых ключей в глобальной адресной книге. Поэтому для создания сертификатов открытых ключей должен использоваться внешний центр сертификации.

3. Для хранения сертификатов открытых ключей абонентов используйте локальную или общую (корпоративную) папку **Контакты**.

Настройка Outlook 2002/2003

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

Установки S/MIME (mailte	st@cryptopro.r	τu)	
Формат сообщения:	S/MIME		2
 Настройка безопасност Настройка по умол Метки безопасности 	ги по умолчани ичанию для все Создать	ию для этого ф ех сообщений Удалить	ормата
ертификаты и алгоритмы —			
Сертификат подписи:	mailtest		Выбрать
Алгоритм хеширования:	, [*	
Сертификат шифрования:	mailtest		Выбрать
21 A	1	-	

Выберите личные сертификаты, соответствующие ключам подписи и шифрования, используя кнопку **Выбрать**. 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 ранее, в диалоге выбора сертификата отображаются только сертификаты, имеющие совпадающий адрес электронной почты и

разрешенные для защиты электронной почты. Выберите пункт меню Сервис, Параметры... и нажмите на закладкуБезопасность. В отображаемом диалоге можно включить режимы Шифровать содержимое и вложения исходящих сообщений и

Добавлять цифровую подпись к исходящим сообщениям 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.

and the second second							?
Настройки	на	астройка поч	нты	Сообщен	ие	Орфо	ография
Безопасн	ость	A	lополнитель	но)	Г	редстави	тели
зопасность эл	ектронной п фровать сод Бавлять циф правлять по, здомлять о п лчанию:	очты цержимое и в ровую подпі дписанные с проверке без /становки S/	вложения исх ись к исходя ообщения от опасности в /MIME (mailte	кодящих сос щим сообще пкрытым тек сех подписа st@cryptopre	бщений ниям стом чных сооб p.ru)	цений S/M	IIME раметры,,
зопасность со Зоны б содеря	держимого езопасности кимого в соо	і позволяют бшениях НТГ	определить ML. Выберит	порядок заг те зону безог	іуска сцен. Іасности Іг	ариев и ак aternet Exr	тивного
зопасность со Зоны б содеря Зона:	держимого іезопасности кимого в соої	і позволяют бщениях НТГ ниченные уз	определить МL. Выберит лы	порядок заг е зону безог	іуска сцен іасности Іг Наст	ариев и ак nternet Exp ройки зоні	стивного plorer, ы
зопасность со Зоны б содерх Зона: фровые удост Дифро обеспе	держимого iesoпасности кимого в соо © Огра товерения (с вые удостов чивают безо	позволяют бщениях НТГ ниченные уз ертификать зерения или опасность ва	определить ML, Выберит лы () сертификата ших электро	порядок заг е зону безог э являются онных транз	пуска сцен пасности Ir Наст документа акций,	ариев и ак hternet Exp ройки зоні іми, котор	тивного blorer, ы
зопасность со Зоны б содер» Зона: фровые удост Дифро обеспе	держимого iesoпасности кимого в соо бо огра огра огра огра огра огра огра огра	позволяют бщениях НТМ ниченные уз ертификать зерения или опасность ва от/экспорт у	определить ML. Выберит лы () сертификаті аших электро достоверені	порядок заг е зону безог э являются онных транз	асности Іг Наст Наст документа акций,	ариев и ак hternet Exp ройки зоні ми, котор удостове	стивного plorer, ы ые рение,
зопасность со Зоны б содер» Зона: фровые удост Цифро обеспе	держимого iesoпасности кимого в соо © Огра огра огра огра огра огра огра огра о	позволяют бщениях НТГ ниченные уз ертификать верения или опасность ва от/экспорт у Опубл	определить ML, Выберит лы i) сертификати ших электро достоверени иковать в гл	порядок заг те зону безо э являются онных транз ий	пуска сцен пасности Ir Наст документа акций. Получить писке адре	ариев и ак hternet Exp ройки зон ми, котор удостове	стивного blorer, ы ые фение

В этом же диалоге дополнительно можно установить опцию **Отправлять подписанные сообщения открытым текстом.** При включенном режиме подпись формируется в виде одного отдельного вложения для всех вложений.

Если режим выключен - сообщения и все вложения будут объединены в единое вложение с включенной в него цифровой подписью.

Отправка подписанных сообщений

Для создания и отправки подписанного сообщения нажмите кнопку **Создать** 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 нажмите кнопку, затем кнопку **Параметры безопасности**, и в отображаемом диалоге установите флаг **Добавить в сообщение цифровую подпись.**

Пара	аметры сообщения				? 🗵
Нас Г	тройка сообщения Важность: Обычная Пометка: Обычное аметры голосования и отсле	Безопас Безопас С С С С С С С С С С С С С	ность Изменение паран Параметры бе	четров безопасности эзопасности	сообщения.
Пар 🕎	Свойства безопасност Шифровать содержимо Абавить в сообщение Не шифровать под Уведомить о пров Параметры безопасности Настройка безопасности	и е и вложения сооб цифровую подпис пись сообщения ерке безопасности	щений ь этого сообщения		
ĸ	<Авто> Метка безопасности Модуль политики: Классификация: Метка: конфиденциальности:	<het></het>	Изменит	настроить	Закрыть
			ок	Отмена й	1 1 1

После того, как сообщение подготовлено к отправке, нажмите кнопку Отправить.

😼 test - Coo	бщение - Microsof	t Word					
	ка <u>В</u> ид Вст <u>а</u> вка	Фор <u>м</u> ат	Сервис	<u>Т</u> аблица	<u>О</u> кно <u>С</u> правка		×
1 🖻 🖨 📓	8860.7	Pa 🛍	× -	🍓 🗔 🛛 1	00% 🔸 📿 🌺 Ari	al	• »
📃 Отправит <u>і</u>	2 Учетные записи 🕶	0 • 0	0 🕵	1 + 4	Параметры	+ HTML	-
📴 Кому	somebody				a ili a mana data sa ta		
📴 Копия	1						
тема:	test						
something							-
							_
Стр. Р	азд	Ha	CT	Кол	ЗАП ИСПР ВДЛ	ЗАМ англий	іский 💋

Если сертификат, с помощью которого подписано сообщение, был отозван, то появится следующее предупреждение, а само сообщение не будет отправлено.

Недол	устимый сертификат		
1	Недопустимый сертификат не подписать или зашифровать (е позволил Microsoft сообщение.	Outlook
		ОК	Справка

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 к контактам.** В отображаемом диалоге нажмите на закладку **Сертификаты** и убедитесь в наличии сертификата отправителя.



После этого нажмите на кнопку **Сохранить и закрыть.** Если абонент с таким адресом уже существует, программа предложит либо **добавить данный контакт как новый**, либо **обновить существующий контакт.** Выберите пункт обновить существующий контакт. При этом в существующий контакт будет добавлен полученный сертификат. Если контакт до этого содержал сертификат, новый сертификат станет использоваться по умолчанию.

Отправка шифрованных сообщений

Для создания и отправки шифрованного сообщения нажмите кнопку **Создать** 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 нажмите кнопку , затем кнопку **Параметры безопасности**, и в отображаемом диалоге установите флаг **Шифровать содержимое и вложения сообщений**. 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.

Проверка сертификата на отзыв

Для контроля проверки сертификатов на отзыв выполните следующие действия.

Откройте полученное подписанное письмо. Нажмите кнопку – признак подписанного сообщения. Если сертификат действительный и не был отозван, то откроется окно, подобное этому:

Свойства безопасности сообщения 🛛 🛛
Prema: test
Сообщения могут содержать шифрование и слои цифровых подписей. Каждый слой допускает наличие нескольких подписей.
✓ Тема: test ✓ Уровень цифровых подписей
🦾 🗸 Подписано: zhenya@cryptopro.ru
Описание:
ОК: подписанное сообщение.
🔽 Всегда предупреждать об ошибках защищенной почты.
Изменить доверие, Подробности Закрыть

Следующее предупреждение означает, что СОС не установлен либо срок его действия истек. Обновите СОС, хранящийся в локальном справочнике сертификатов, с использованием доступных средств.

Свойства безопасности с	ообщения	? 🛛
Tema: RE: 1ef		1
Каждый слой допускает налич	ифрование и слои ци ние нескольких подп	юровых подписеи. исей.
🗸 Тема: RE: 1ef		
🖉 🗸 Уровень цифровых под	дписей	
— 🔼 Подписано: mailtest	t@cryptopro.ru	
Описание:		
является сертификат недо истек.	оступным, либо срок	его деиствия
подписано mailtest@cryptopro. 2001/ГОСТ Р 34.11-94 в 16:52:	ru с помощью ГОСТ Р 22 19.03.2007,	² 34.10-
🔽 Всегда предупреждать об о	ршибках защищенной	й почты.
Internet to a second second	1	
Изменить доверие	Подробности	Закрыть

Если же СОС обновлен, то при открытии письма, подписанного отозванным сертификатом, появится следующее предупреждение:



Нажмите кнопку Сведения для просмотра сведений о сертификате:

Своиства безопасности с	сообщения	? ×
Tema: test Cooбщения могут содержать I Каждый слой допускает нали	шифрование и слои циф уче нескольких подпи	фровых подписей. сей.
О Тема: test О Уровень цифровых по О Подписано: mailtes	идписей st@cryptopro.ru	
Описание:		
Описание: Ошибка: •Использованный для созд находится в допустимом	ания данной подписи о списке отмененных сер	сертификат
Описание: Ошибка: •Использованный для созд находится в допустимом по вписано mailtest@cryptopro Всегда предупреждать об	ания данной подписи о списке отмененных сер им с помошью БОСТ Р ошибках защищенной	сертификат ітификатов. за то. почты.