



КИТ-Журнал

Компания Информационных Технологий

Служба штампов времени

Руководство пользователя

Оглавление

О программе	3
Системные требования	4
Установка Службы штампов времени	5
Установка Сертификата Службы штампов времени.....	5
Удаление Службы штампов времени.....	6
Принцип работы	7
Журнал Службы штампов времени	8
Приложение.....	10
Установка сертификата «КриптоПро CSP» в личное хранилище локального компьютера	10
Установка сертификата «ViPNet CSP» в личное хранилище локального компьютера	11



О программе

Служба штампов времени - это компонент программного обеспечения КИТ-Журнал, который позволяет создавать доказательство факта существования электронного документа на определённый момент времени. Штамп времени — это подписанный ЭЦП документ, которым Служба штампов времени удостоверяет, что в указанный момент времени ей было предоставлено значение хэш-функции от другого документа. Само значение хэш-функции также указывается в штампе.

Таким образом, с помощью штампа времени вы обеспечиваете невозможность отказа автора документа от своей подписи.

Наличие штампа времени в подписанном документе позволяет продлевать срок действия электронной подписи. Штамп времени удостоверяет, что подпись была создана до того, как сертификат ключа подписи был аннулирован (отозван). Таким образом, для проверки подписи, созданной до момента отзыва сертификата, можно использовать уже отозванный сертификат.

Цепочка штампов времени позволяет создавать системы архивного хранения электронных документов, сохраняющие актуальность ЭЦП в документах. В ином случае, актуальность подписанного документа ограничена сроком действия сертификата ключа подписи и сроком действия сертификата на СКЗИ (средство криптографической защиты информации), использованное для создания оригинальной подписи документа.

Служба штампов времени должна быть доверенным субъектом Инфраструктуры открытых ключей, который обладает точным и надёжным источником времени.

Значение хэш-функции от документа, на который получен штамп времени, служит для связи штампа с документом.

Служба штампов времени программного обеспечения КИТ-Журнал не предоставляет сетевых сервисов, она самостоятельно общается с базой данных журналов (в том числе и по сети), обнаруживает и подписывает ЭЦП субъектов.

Для работы Службы штампов времени необходим сертификат подписи.



Системные требования

Компонент	Требования
Операционная система	32-битные версии Windows Server 2003; Windows XP; Windows Vista, Windows 7 с последними пакетами обновлений. 64-битные версии Windows с поддержкой WoW64.
Процессор	Процессор, совместимый с Pentium III, или выше
Память	Не менее: 256 МБ
Программное обеспечение	Microsoft SQL Server 2008 R2 Native Client MS XML 4.0 или выше




Установка Службы штампов времени

Установка Службы штампов времени сводится к выбору нужных компонентов установочного пакета для сервера и следованию инструкциям мастера установки Службы штампов времени. Для запуска мастера установки Службы штампов времени запустите «STSSetup.exe» с установочного диска.

При установке необходимо указать: экземпляр SQL сервера, базу данных, адрес сервера, учетные данные администратора. Права администратора требуются для создания учетной записи для Службы штампов времени на SQL сервере.

Установка Сертификата Службы штампов времени

Служба штампов времени работает с сертификатами, установленными в Личное хранилище Локального компьютера. В зависимости от криптопровайдера, установка сертификата в личное хранилище может различаться. В приложении есть инструкции по установке сертификата для криптопровайдера КриптоПро¹ и VipNet².

Выбор сертификата для Службы штампов времени осуществляется через программу управления службой. Запустите программу управления «Пуск» - «КИТ-Журнал» - «Служба штампов времени КИТ-Журнал». В панели задач появится значок программы управления . Нажмите правой кнопкой мыши на значок, в контекстном меню значка выберите пункт «Установить сертификат штампа времени». В появившемся окне запроса сертификата выберите нужный сертификат.

Служба штампов времени будет постоянно использовать закрытый ключ выбранного сертификата для создания подписи, поэтому для нормальной работы службы необходимо, чтобы закрытый ключ сертификата всегда был доступен. Если закрытый ключ находится на сменном носителе, он должен быть подключен к компьютеру. А пароль и пинкод для доступа к закрытому ключу сохранены на компьютере при установке сертификата.

¹ Данное торговое название и права на него принадлежит его обладателю и никак не связаны с разработчиками программного обеспечения КИТ-Журнал.

² Данное торговое название и права на него принадлежит его обладателю и никак не связаны с разработчиками программного обеспечения КИТ-Журнал.



Удаление Службы штампов времени

Удаление Службы штампов времени происходит стандартными средствами операционной системы через соответствующий пункт «Установка и удаление программ» меню «Панели управления» или через соответствующий пункт меню «Пуск» - «Программы» - «КИТ-Журнал».



Принцип работы

Служба штампов времени периодически подключается к базе данных с журналами и проверяет наличие не заверенных ЭЦП, после чего они заверяются штампом времени текущего сертификата Службы Штампов Времени.

После смены сертификата Службы штампов времени все ЭЦП в журналах вместе со старыми штампами времени заверяются новым штампом. В результате получается цепочка штампов времени, в которой каждый штамп времени удостоверяет, что предыдущий штамп, а в конечном счете и ЭЦП документа, был создан до того, как сертификат его ключа подписи был аннулирован (отозван).

Смена сертификата Службы Штампов Времени должна происходить до окончания его срока действия.



Журнал Службы штампов времени

Служба штампов времени ведет лог своих действий в системном журнале «Security Journals - TimeStamp Service». Далее приводится описание всех сообщений и возможные причины их возникновения.

Сообщение: «Ошибка подключения».

Описание: Ошибка при подключении к базе данных.

Возможные причины: неверные данные для подключения: адрес сервера, данные учетной записи; отсутствует база данных. Причина ошибки указана в тексте сообщения.

Сообщение: «Служба запущена».

Описание: Успешный запуск службы штампов времени.

Сообщение: «Ошибка при получении списка таблиц».

Описание: Ошибка при попытке получить список журналов из базы данных.

Возможные причины: Причина ошибки указана в тексте сообщения.

Сообщение: «Ошибка при заверении подписи».

Описание: Ошибка при попытке заверить подпись.

Возможные причины: Неверно установленный сертификат; отсутствие закрытого ключа сертификата подписи. Причина ошибки указана в тексте сообщения.

Сообщение: «Не удалось изменить запись».

Описание: Ошибка при попытке записать подпись в Журнал.

Возможные причины: Причина ошибки указана в тексте сообщения.

Сообщение: «Подпись заверена».

Описание: Подпись была успешно заверена.



Сообщение: «Ошибка получения 1-го сертификата подписи сообщения».

Описание: Возникла ошибка при попытке получить сертификат подписи.

Возможные причины: Причина ошибки указана в тексте сообщения.

Сообщение: «Ошибка получения сертификатов подписи».

Описание: Возникла ошибка при попытке получить доступ к сертификату подписи.

Возможные причины: Причина ошибки указана в тексте сообщения.



Приложение

Установка сертификата «КриптоПро CSP» в личное хранилище локального компьютера

Вам необходимы:

1. Файл с сертификатом, обычно этот файл передаёт вам ваш УЦ, где вы получали сертификат.
2. Установленный криптопровайдер «КриптоПро CSP»³.

Найдите в Пуске группу программы «Крипто-Про». В группе запустите «КриптоПро CSP».

В открывшемся окне «Свойства КриптоПро CSP» выберите вкладку «Сервис». В группе элементов «Личный сертификат» нажмите на кнопку «Установить личный сертификат...». После этого откроется «Мастер установки личного сертификата». На второй странице мастера необходимо указать файл с вашим сертификатом. На следующей вкладке отображается краткая информация о субъекте выбранного сертификата, а также есть возможность посмотреть все свойства сертификата. На следующей странице необходимо указать имя ключевого контейнера и выбрать пункт «Введенное имя задаёт ключевой контейнер: Компьютера». В контейнере содержится ваш закрытый ключ.

Обычно данный ключ формируется на этапе запроса сертификата в УЦ и, в зависимости от УЦ, передаётся вам на носителе (гибкий диск, флеш-диск, электронные ключи), либо данный ключ формируется пользователем при запросе и остается у него, также на каком-либо носителе или сохраненным в компьютере.

Вставьте ваш ключевой носитель и нажмите кнопку обзор. Появится список всех найденных ключевых контейнеров, вам необходимо выбрать свой. При запросе пароля к закрытому ключу поставьте галочку «Запомнить пароль». При запросе хранилища сертификатов выберите «Личное». Завершите установку сертификата, следуя инструкции мастера.

За дополнительной информацией об установке личного сертификата обращайтесь в УЦ и к производителю криптопровайдера.

Проверить наличие сертификата в Личном хранилище локального компьютера можно с помощью утилиты КриптоПро «Сертификаты». Открыть утилиту можно через Пуск. Найдите в Пуске группу программы «Крипто-Про». В группе запустите «Сертификаты». В окне сертификатов откройте пункт «Сертификаты (локальный компьютер)», подпункты «Личное», «Реестр», «Сертификаты». В правой части отобразится список установленных сертификатов, в личном хранилище сертификатов локального компьютера.

³ Данный материал относится к версии 3.6



Установка сертификата «ViPNet CSP» в личное хранилище локального компьютера

Вам необходимы:

1. Файл с вашим сертификатом, обычно этот файл передаёт вам ваш УЦ, где вы получали сертификат.
2. Установленный криптопровайдер «ViPNet CSP»⁴.

Найдите в Пуске группу программы «ViPNet». В группе запустите «Настройка криптопровайдера ViPNet CSP».

В открывшемся окне «Настройка ViPNet CSP» выберите в списке слева пункт «Контейнеры». В открывшей области нажмите на кнопку «Установить сертификат из файла». В диалоге выбора сертификата найдите и укажите файл с вашим сертификатом. После этого откроется «Мастер установки сертификатов». На второй странице мастера необходимо указать, что Сертификат будет установлен в хранилище сертификатов компьютера. А также отметить галочку «Установить сертификаты издателей».

На следующей странице необходимо отметить галочку «Указать контейнер с закрытым ключом», иначе сертификат будет невозможно использовать в программе.

Далее мастер предложит окно выбора контейнера с закрытым ключом. Контейнеры в ViPNet хранятся в файлах на дисках, обычно располагаются в корневой папке диска «\Infotecs\Containers». При запросе пароля к закрытому ключу поставьте галочку «Сохранить пароль».

При необходимости вставьте ваш ключевой носитель. Нажмите кнопку обзор, найдите и укажите папку с вашим ключевым контейнером. В списке контейнеров выберите свой контейнер. И завершите установку сертификата, следуя инструкции мастера.

За дополнительной информацией об установке личного сертификата обращайтесь в УЦ и к производителю криптопровайдера.

Проверить наличие сертификата в Личном хранилище локального компьютера можно с помощью «Консоли управления (MMC)». Открыть консоль можно через Пуск. В ОС до версии Windows 7: «Пуск» - «Выполнить», в открывшемся окне набрать «mmc» и нажать на кнопку «ОК». В ОС Windows 7: нажать на «Пуск» и набрать «mmc», в появившемся списке выбрать «mmc.exe». Откроется окно консоли.

В окне консоли выберите пункт главного меню «Файл» - «Добавить или удалить оснастку». В списке «Доступные оснастки» выберите «Сертификаты» и нажмите кнопку «Добавить». В появившемся окне выберите пункт «учетной записи компьютера». Нажмите на кнопку далее. И на следующей странице кнопку «Готово». В окне добавления оснасток нажмите кнопку «ОК». В консоли откройте пункт «Сертификаты (локальный компьютер)», подпункты «Личное»,

⁴ Данный материал относится к версии 3.2(2.7965)



«Сертификаты». В правой части отобразится список установленных сертификатов, в личном хранилище сертификатов локального компьютера.

