



Trusted Java 1.5.2

Описание по установке



Цифровые технологии ®

2009 год

Настоящий документ содержит описание операций по установке и настройке криптопровайдеров КриптоПро CSP и Trusted Java.

Руководство предназначено для администраторов системы. В нем содержится информация, необходимая для установки, настройки и эксплуатации Trusted Java, а также описание функциональных возможностей программного продукта.

По всем вопросам обращайтесь [в службу технической поддержки](#) или [на форум компании-разработчика](#)

Новинки версии

Версия Trusted Java 1.5.2 включает в себя как совершенно новые, так и оптимизированные по сравнению с более ранними версиями, функциональные возможности.

- обеспечена совместимость JSSE с веб-сервером Apache Tomcat 5.5;
- добавлены новые классы для обеспечения совместимости XMLSig с MS XML;
- оптимизирована подпись группы файлов на одном ключе;
- добавлена возможность получения списка ключевых контейнеров, подключенных к системе.

Общие сведения

Программный продукт Trusted Java является средством криптографической защиты информации и представляет собой набор криптоалгоритмов, реализованных в соответствии с требованиями архитектур JSSE и JCE.

Провайдер JSSE обеспечивает организацию защищенного взаимодействия по протоколам SSL и TLS с использованием российских криптографических алгоритмов. Таким образом, он даёт возможность устанавливать безопасные интернет-соединения и обеспечивать защиту канала передачи данных. Кроме того, компонент включает функциональность для шифрования данных, аутентификации клиента и сервера и целостности сообщений.

Провайдер JCE является криптографическим расширением Trusted Java, т.е. позволяет реализовать российские алгоритмы криптографических преобразований для обеспечения работы с сертификатами, создания и проверки корректности электронной цифровой подписи и шифрования данных.

ПО Trusted Java обеспечивает возможность поддержки российской криптографии в соответствии с положениями российского законодательства.



Для авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями используются функции формирования и проверки электронно-цифровой подписи, для обеспечения конфиденциальности информации и контроля ее целостности – шифрование и имитозащита.

Также Trusted Java позволяет работать с сертификатами и запросами на сертификат, создавать и проверять корректность электронной цифровой подписи данных, шифровать данные, загружать Java апплеты по протоколу TLS на криптографических алгоритмах ГОСТ.

Используемые сертифицированные российские криптоалгоритмы предназначены для:

авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями (создание и проверка ЭЦП).

обеспечения конфиденциальности и контроля целостности информации (шифрование и имитозащита).

Библиотека Trusted Java предназначена, прежде всего, для системных интеграторов и разработчиков прикладных и бизнес-систем для решения вопросов информационной безопасности и юридической значимости электронного документооборота. При работе с банковскими клиент-серверными системами, защищенными электронными торговыми площадками и другими бизнес-приложениями, написанными на Java, требуется поддержка шифрования, электронной цифровой подписи, строгой аутентификации в соответствии с положениями российского законодательства. ПО Trusted Java позволяет использовать эти возможности.

Состав продукта

В состав программного продукта входит:

Провайдер JSSE

Документация

- Руководство администратора
- Руководство разработчика
- Описание новинок версии

Лицензионное соглашение



Приложение "Удалить"

Программа управления лицензиями (только для ОС Windows)

Функциональные возможности продукта

Библиотека Trusted Java реализует в Java-приложениях сертифицированные криптографические алгоритмы, предоставляемые криптопровайдером КриптоПро CSP от компании «Крипто-ПРО».

Функциональные возможности	Направления работы	Возможные операции
Поддержка криптографических алгоритмов	ГОСТ 28147-89 (шифрование)	Предназначен для обеспечения конфиденциальности информации и контроля ее целостности посредством шифрования имитозащиты
	ГОСТ Р 34.11-94 (хеширование) ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 (ЭЦП)	Предназначены для авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями. Это достигается благодаря использованию процедур создания ЭЦП проверки ЭЦП
Работа с сертификатами и запросами на сертификат	Операции с цифровыми сертификатами	создание сертификата установка сертификата в хранилище работа со списками отзыванных сертификатов (COC) поддержка CMS поддержка TSP поддержка OCSP
		Операции с запросами на



	сертификат	сертификат
Криптографические операции	Электронная цифровая подпись (ЭЦП) данных	создание ЭЦП проверка корректности ЭЦП по сертификату создание ЭЦП в XML документах проверка ЭЦП в XML документах
	Шифрование	шифрование данных
Загрузка Java-апплетов	возможность загрузки Java-апплетов по ГОСТ TLS для Internet Explorer 6 (и выше) с установленным Sun Java Plugin 1.5 (и выше)	
Поддержка JCE и JSSE	провайдер JCE	поддержка ГОСТ-алгоритмов в протоколе на стороне Сервера поддержка двухфакторной аутентификации по ГОСТ сертификатам на стороне Клиента поддержка прокси на стороне Клиента
	провайдер JSSE	поддержка ГОСТ в TSP

Требования к программному обеспечению

Для установки и функционирования программного продукта Trusted Java необходимы следующие компоненты:

- Операционная система Windows 2000/2003/XP;
- Установленный дистрибутив криптопровайдера КриптоПро CSP v. 3.0;
- Java 2 (Sun JDK 1.5).

Установка ПО

В главе Установка ПО содержится информация, необходимая для установки и первоначальной настройки обязательных для корректной работы ПО составляющих: криптопровайдера КриптоПро CSP и, непосредственно, самого программного продукта Trusted Java



Установка дистрибутива ПО СКЗИ КриптоПро CSP

Процедура установки криптопровайдера КриптоПро CSP проходит в 3 этапа

- ознакомление с требованиями к системе
- установка дистрибутива ПО СКЗИ КриптоПро CSP
- изменение набора устройств хранения ключевой информации

Установка дистрибутива должна производиться пользователем, имеющим права администратора.

Перед установкой дистрибутива ПО СКЗИ КриптоПро CSP удалите все ранее существующие версии устанавливаемого ПО.

Если модуль криптографической поддержки не удален, новая версия не будет установлена.

Для удаления ранее установленного ПО СКЗИ КриптоПро CSP используйте пункты основного меню Windows Пуск -> Панель управления -> Установка и удаление программ.

Для установки ПО запустите на исполнение файл дистрибутива. Далее следуйте стандартным инструкциям программы InstallShield Wizard.

После завершения установки дистрибутива перезагрузите компьютер.

Изменение набора устройств хранения ключевой информации

При инсталляции программного обеспечения по умолчанию устанавливаются все модули, обеспечивающие работу с различными поддерживаемыми устройствами хранения ключевой информации, но при этом настройки СКЗИ КриптоПро CSP допускают использовать в качестве ключевого носителя только дискету 3,5".

Если для работы с ПО СКЗИ необходимы дополнительные типы устройств работы с ключевыми носителями, выберите режим изменения их состава. Для этого:

Откройте панель управления компьютером, используя пункты меню Пуск -> Панель управления.

В окне панели управления выберите значок КриптоПро CSP.

В панели настройки СКЗИ КриптоПро CSP выберите закладку Оборудование и, нажав кнопку Настроить считыватели..., добавьте (или удалите) из списка

те устройства, которые будут (или не будут) использованы в качестве считывателей ключевой информации.

Установка лицензии

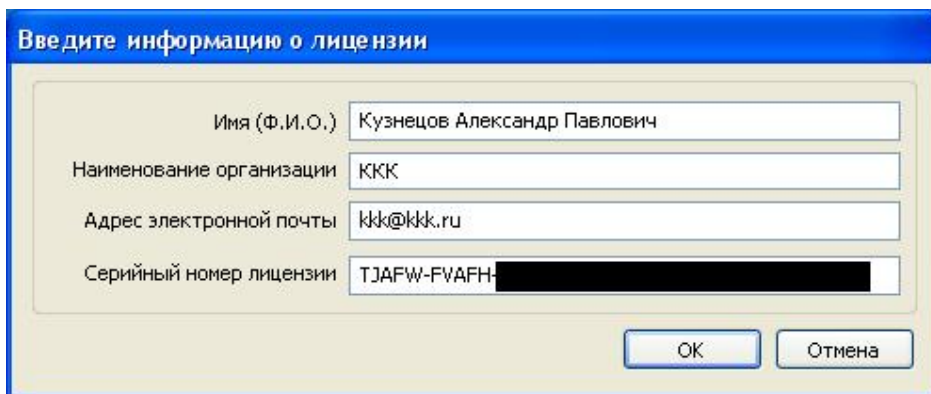
Процедура регистрации программного продукта различается в зависимости от операционной системы.

Чтобы зарегистрировать программный продукт Trusted Java в ОС Windows:

Откройте окно Управление лицензиями (Программы > Digt > Trusted Java 1.5.1 > Управление лицензиями). При установке ПО Trusted Java это окно появляется автоматически.

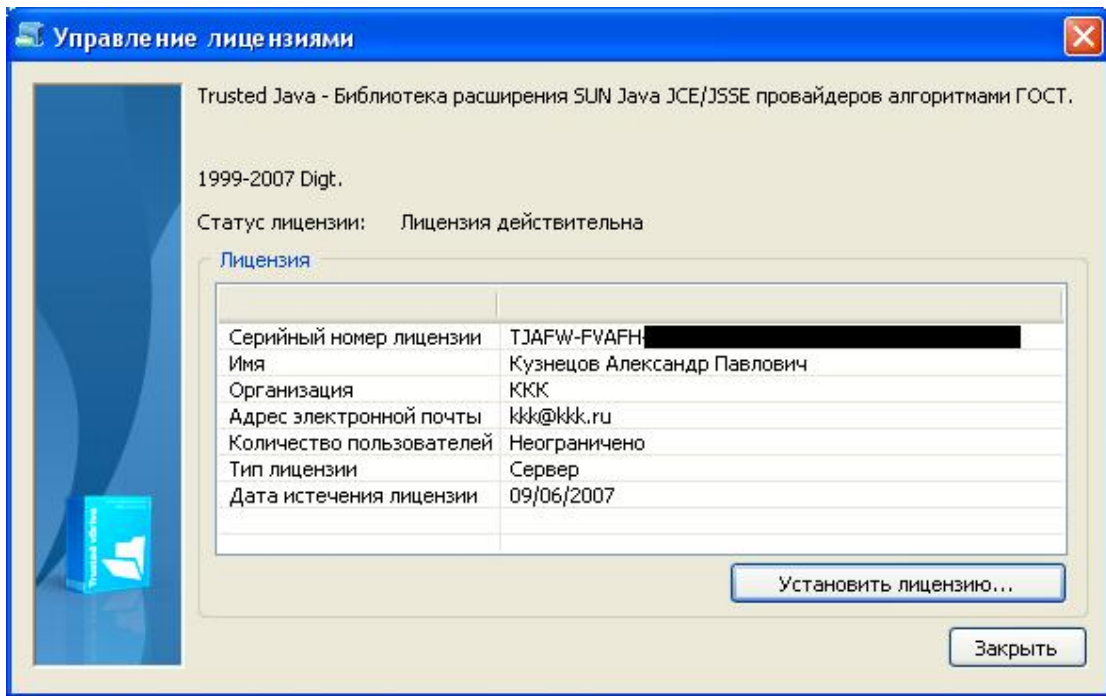
В этом окне нажмите на кнопку Установить лицензию

В открывшемся окне введите информацию о лицензии согласно выданным вам документам



Введите информацию о лицензии	
Имя (Ф.И.О.)	Кузнецов Александр Павлович
Наименование организации	ККК
Адрес электронной почты	kkk@kkk.ru
Серийный номер лицензии	TJAFW-FVAFH- [REDACTED]

При успешной регистрации ПО Trusted Java статус лицензии изменится на "Действительна" (см. в окне Управление лицензиями - > Статус лицензии):



В поле Лицензия отображается информация в соответствии с используемой лицензией на программный продукт Trusted Java:

- серийный номер лицензии
- имя администратора системы
- наименование организации, использующей данное ПО
- адрес электронной почты
- количество пользователей
- тип лицензии
- дата истечения срока действия лицензии на программный продукт

Чтобы зарегистрировать программный продукт Trusted Java в других ОС, необходимо выполнить следующие действия:

В дистрибутиве ПО существует файл `license.lic`, расположенный в каталоге `/opt/DIGT/etc/Trusted/Java 1.5.2/license.lic`. Откройте файл

С помощью текстового редактора впишите выданную вам лицензию в поле `SerialNumber`.

При удачном выполнении операции система сообщит о том, что введенная лицензия действительна.

Удаление ПО

В этой главе руководства рассматриваются вопросы удаления программного обеспечения, а именно:

- удаления криптопровайдера КриптоПро CSP
- удаления ПО Trusted Java

Удаление ПО Trusted Java

Удалить ПО Trusted Java можно тремя способами:

- с помощью программы установки
- стандартными средствами ОС Windows
- с помощью функционального меню каталога Trusted Java

Для удаления программы Trusted Java с помощью программы установки:

Запустите на исполнение файл дистрибутива и следуйте стандартным инструкциям программы InstallShield Wizard

Откроется окно Обслуживание программы: поставьте флаг в поле Удалить и нажмите на кнопку Далее

Возникнет сообщение с предложением выполнить процедуру удаления: нажмите на кнопку Удалить

Начнется процесс удаления ПО Trusted Java. Нажмите кнопку Готово

Для удаления программы Trusted Java стандартными средствами ОС Windows

Откройте Пуск - > Панель управления, выберите опцию Установка и удаление программ

В списке выберите запись Trusted Java 1.5.1 и нажмите на кнопку Удалить и подтвердите решение об удалении

Начнется процесс удаления ПО. По завершении процесса библиотека Trusted Java будет удалена с компьютера и из списка элементов Установленные программы

Для удаления программы Trusted Java с помощью функционального меню выберите приложение Удалить в каталоге установленного ПО Trusted Java. Приложение Удалить расположено здесь:

Пуск - > Программы - > Digt - > Trusted Java 1.5.1 - > Удалить.

Часто задаваемые вопросы

Вопрос	Ответ
Java сообщает, что не найден провайдер DIGT	Добавьте в начало кода строку: Security . addProvider (new DIGTProvider ())
Ошибка : java.lang.UnsatisfiedLink Error: no djcpNNN in java.library.path	Java не может найти библиотеку. Поместите ее по одному из путей переменных окружения %PATH% либо укажите путь к ней с помощью параметра java машины - Djava.library.path.
Я не встретил описания моей проблемы, как быть?	Стоит проверить, не истек ли период использования Крипто Про CSP. В ином случае опишите сложившуюся ситуацию с примерами появившихся ошибок и отправьте письмо разработчику: support@digt.ru

Техническая поддержка

По вопросам технической поддержки ПО Trusted Java обращайтесь:

По электронной почте: support@trusted.ru

По телефонам: (8362) 55-62-81, (8362) 55-62-27

По адресу: 424019, Россия, Республика Марий Эл, г. Йошкар-Ола, ул. Фестивальная, д.73

Систематическое техническое сопровождение организаций по вопросам работы с ПО Trusted Java осуществляется при условии оплаты стоимости годового пакета технических услуг. В течение этого срока разработчик бесплатно поставляет новые реализации продукта в рамках приобретенной версии. Новые версии продукта поставляются в соответствии с прайс-листом.

О компании-разработчике



Компания «Цифровые технологии» – российский разработчик и поставщик программного обеспечения в области защиты информации, систем электронного документооборота и хранения данных. Основной сферой деятельности компании является разработка, внедрение и поддержка криптографических продуктов и решений для государственных и коммерческих структур.

Телефон: (8362) 55-62-81

Факс: (8362) 55-62-27

Интернет: <http://www.trusted.ru>

E-mail: info@trusted.ru

