



Памятка пользователю Удостоверяющего центра InfoTrust

Поздравляем Вас с получением Вашего персонального сертификата ключа подписи!

Сертификат ключа подписи, выданный Вам как его владельцу, выпущен Удостоверяющим центром InfoTrust в полном соответствии с законом от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи». Криптографические алгоритмы, с которыми может быть использован Ваш сертификат, соответствуют требованиям российских ГОСТов и реализуются сертифицированными в установленном порядке средствами криптографической защиты информации (СКЗИ КриптоПро CSP и совместимыми с ним).

Удостоверяющий центр InfoTrust ООО НПП «Ижинформпроект» является официально зарегистрированным в Едином государственном реестре сертификатов ключей подписей уполномоченных лиц удостоверяющих центров Уполномоченного федерального органа в области электронной цифровой подписи. ООО Научно-производственное предприятие «Ижинформпроект» осуществляет свою деятельность на территории Российской Федерации на основании соответствующих лицензий ФСБ России и Минсвязи России.

Выпуская сертификат на Ваше имя, Удостоверяющий центр выступает в качестве третьей доверенной стороны защищенного электронного взаимодействия и подтверждает, что открытый криптографический ключ, указанный в Вашем сертификате принадлежит Вам и соответствует закрытому ключу, имеющемуся только у Вас на защищенном ключевом носителе. Кроме того, в сертификате в соответствии с требованиями закона «Об ЭЦП» указывается необходимая информация, позволяющая идентифицировать Вас как участника защищенного электронного взаимодействия.

С помощью сертификата Вы можете совершать юридически значимые действия в системах электронного документооборота и, в зависимости от профиля Вашего сертификата, и в распределенных вычислительных системах (Internet). При этом Вам доступны многие защищенные сервисы, предоставляемые современными информационно-телекоммуникационными системами: защита соединений в Интернете для проверки подлинности сервера и клиента, защищенная электронная почта (электронная цифровая подпись и шифрование), компоненты с электронной цифровой подписью (ЭЦП электронных документов) и т.п.

Вы должны осознавать, что все функции сертификата могут быть обеспечены только **при условии сохранения Вами в тайне Вашего закрытого ключа** на ключевом носителе. В связи с этим, особо обращаем Ваше внимание на некоторые правила пользования сертификатом.

— **Выбор носителя.** Базовым носителем ключей является магнитный диск. 3,5”. Для надежного хранения закрытого криптографического ключа рекомендуется использовать специально предназначенные для этих целей устройства (eToken, ruToken и т.п.). Хранение закрытых криптографических ключей в виде файлов в операционной системе (реестр Windows) допускается только в случае принятия дополнительных мер по обеспечению защиты компьютера от несанкционированного доступа с помощью сертифицированных в установленном порядке средств.

— **Хранение ключей.** Носители ключей необходимо хранить в условиях, исключающих доступ к ним посторонних лиц (сейф, металлический шкаф, персональный ящик и т.п.).

— **Использование.** Для безопасного использования криптографических ключей рекомендуется принять меры по оборудованию, охране и организации режима в помещении, где установлены СКЗИ и хранятся ключевые документы.

— **Взаимодействие с УЦ.** Пользователь должен незамедлительно сообщать в установленном порядке о фактах доступа (вероятного доступа) к закрытому ключу посторонних лиц. При этом, до выяснения фактов наличия компрометации ключей действие сертификата приостанавливается. В случае, если компрометации ключей не было — сертификат возобновляется, в противном случае — отзывается (аннулируется), с последующим выпуском нового сертификата.

Пользователь должен своевременно сообщать об изменении значимых атрибутов (параметров), в том числе включаемых в сертификат (изменение ФИО, паспортных данных, должности, организации и т.п.).

В соответствии с требованиями российского законодательства **сертификат ключа подписи выдается физическому лицу без права передачи.**

УЦ выпускает сертификаты в соответствии Правилами применения сертификатов УЦ InfoTrust, которые регламентируют применение сертификата для разрешенных приложений и систем с установленными требованиями безопасности, в порядке, определенном Регламентом УЦ InfoTrust. Краткие сведения о содержании этих документов Вы можете получить в Справочнике по Инфраструктуре открытых ключей УЦ InfoTrust.

Более подробную информацию вы можете получить в Удостоверяющем центре InfoTrust ООО НПП «Ижинформпроект» по адресу 426008, г. Ижевск, ул. Бородина, 21, офис 207, тел./факс 918-100, 918-102, www.infotrust.ru, pki@infotrust.ru.