Научно-производственное предприятие
“ИЖИНФОРМПРОЕКТ”

УТВЕРЖДЕНЫ
приказом от 29.10.2018 № 8

Справочник
по Инфраструктуре открытых ключей
Удостоверяющего центра InfoTrust
(PKI Disclosure Statement — PDS)
OID 1.2.643.3.34.1.3

Редакция № 4.4

INFOTRUST
удостоверяющий центр

Ижевск 2018

Настоящий документ разработан в соответствии с рекомендациями RFC 3647 «Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework» и описывает основные условия получения сертификатов в Удостоверяющем центре InfoTrust и порядок их использования в различных приложениях Инфраструктуры открытых ключей.

Общество с ограниченной ответственностью научно-производственное предприятие «Ижинформпроект» (ООО НПП «Ижинформпроект»), предоставляющее услуги *Удостоверяющего центра* в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», именуемое в дельнейшем «*Удостоверяющий центр*», зарегистрировано на территории Российской Федерации в городе Ижевске.

Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий:

1 лицензия Управления ФСБ России по Удмуртской Республике на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) от 11.10.2016 № 110Н;

2 лицензия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) на оказание услуг связи по

передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации, от 18.08.2018 № 163770;

3 лицензия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) на оказание телематических услуг связи от 18.08.2018 № 163771.

Сертификаты уполномоченного лица *Удостоверяющего центра* зарегистрированы в Едином государственном реестре сертификатов ключей подписей уполномоченных лиц удостоверяющих центров, о чем получены соответствующие уведомления Минкомвязи России (Росинформтехнологии):

1 Уведомление № 40 от 13 апреля 2006 г. о регистрации сертификата ключа подписи уполномоченного лица Удостоверяющего центра. Регистрационный номер записи № П44-05-12-32 от 16.03.2006;

2 Уведомление № 136 от 05 октября 2007 г. о регистрации сертификата ключа подписи уполномоченного лица Удостоверяющего центра. Регистрационный номер записи № П44-05-12-134 от 03.10.2007;

3 Уведомление № 324 от 28 сентября 2009 г. о внесении в Единый государственный реестр сертификатов ключей подписей уполномоченных лиц удостоверяющих центров. Регистрационный номер записи № П44-05-12-324 от 28.09.2009;

4 Уведомление № 767 от 04 октября 2011 г. о внесении в Единый государственный реестр сертификатов ключей подписей уполномоченных лиц удостоверяющих центров. Регистрационный номер записи № П44-05-12-767 от 04.10.2011;

5 Уведомление Минкомсвязи от 16.08.2012 № 996 о внесении в Единый государственный реестр сертификатов ключей подписей уполномоченных лиц удостоверяющих центров.

6 Уведомление Минкомсвязи от 09.10.2012 № 1015 о внесении в Единый государственный реестр сертификатов ключей подписей уполномоченных лиц удостоверяющих центров.

Сертификаты ключа подписи уполномоченного лица *Удостоверяющего центра* включены в Список доверенных удостоверяющих центров общероссийского государственного информационного центра на основании Заключения по итогам оценки соответствия удостоверяющего центра ООО НПП «Ижинформпроект» Требованиям к технологиям, форматам, протоколам информационного взаимодействия, унифицированным программно-техническим средствам подсистемы удостоверяющих центров общероссийского государственного информационного центра (направлено письмом Росинформтехнологии № П44-438 от 08.12.2009, продлено до 30.11.2011).

Удостоверяющий центр InfoTrust присоединен к единой системе удостоверяющих центров в области электронной цифровой подписи:

1 Свидетельство Минкомвязи России № 146 от 10 ноября 2011 г. о присоединении к Единой системе удостоверяющих центров в области электронной цифровой подписи.

Удостоверяющий центр InfoTrust аккредитован в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»:

1 Свидетельство Минкомвязи России № 17 от 19 июля 2012 об аккредитации удостоверяющего центра (на основании Приказа Минкомсвязи России № 182 от 19.07.2012 «Об аккредитации удостоверяющих центров»);

2 Свидетельство Минкомвязи России № 794 от 21 августа 2017 об аккредитации удостоверяющего центра (на основании Приказа Минкомсвязи России № 427 от 21.08.2017 «Об аккредитации удостоверяющих центров»).

Контактная информация

телефон/факс: +7 (3412) 918-100

e-mail: pki@infotrust.ru

WWW: www.infotrust.ru

Одной из главных задач при создании защищенных информационно-телекоммуникационных систем, использующих технологию с открытыми ключами и цифровыми сертификатами, является организация подсистемы Инфраструктура Открытых Ключей (ИОК) — Public Key Infrastructure (PKI), включающей полный комплекс программно-аппаратных средств, а также организационно-технических и административных мероприятий, обеспечивающих необходимый сервис для управления ключами пользователей системы и их сертификатами ключей подписи.

Основным элементом ИОК является Удостоверяющий Центр (УЦ), который в лице уполномоченного лица УЦ обеспечивает контроль за выполнением всех процедур, связанных с формированием, регистрацией, хранением и обновлением ключей, цифровых сертификатов и списков отозванных сертификатов.

Удостоверяющий центр InfoTrust формирует квалифицированные сертификаты ключей проверки электронной подписи (далее – сертификаты) и списки отозванных сертификатов в соответствии с Рекомендациями ITU-T X.509 «Information Technology — Open Systems Interconnection — The Directory: Authentication Framework», RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile» и RFC 3039 «Internet X.509 Public Key Infrastructure Qualified Certificates Profile» с соблюдением требований Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», Гражданского кодекса Российской Федерации, Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и позволяет обеспечить:

— внесение в реестр Удостоверяющего центра регистрационной информации о пользователях;

— изготовление сертификатов пользователей в электронной форме и в виде документа на бумажном носителе;

— ведение реестра изготовленных сертификатов пользователей;

— предоставление копий сертификатов в электронной форме, находящихся в реестре изготовленных сертификатов, по запросам пользователей;

— аннулирование (отзыв), приостановление и возобновление действия сертификатов по обращениям владельцев сертификатов;

— предоставление пользователям сведений об аннулированных и приостановленных сертификатах;

— подтверждение подлинности электронных цифровых подписей в документах, представленных в электронной форме, и в изготовленных сертификатах, по обращениям пользователей.

В основу системы администрирования Удостоверяющего центра положены принципы строгой аутентификации, принятые в Рекомендации ITU-T X.509 v.3 и базирующиеся на свойствах асимметричных криптографических систем. В отличие от симметричных криптосистем, использующих один ключ, криптосистемы с открытым ключом предполагают наличие у пользователя парных ключей — секретного (закрытого) и открытого (общедоступного).

Процедура идентификации и установления подлинности источника информации называется аутентификацией. Аутентификация опирается на наличие у каждого пользователя уникального имени (Distinguished Name в терминологии X.509), отличного от имен всех остальных пользователей, атрибуты которого включаются в сертификат.

За достоверность и правильность информации, включаемой в сертификат, несет ответственность Удостоверяющий центр. С этой целью он запрашивает у пользователей необходимые подтверждающие документы, запрашивает и получает сведения из государственных информационных ресурсов.

Каждый пользователь идентифицируется с помощью своего закрытого ключа. С помощью соответствующего открытого ключа любой пользователь имеет возможность определить, является ли его партнер по связи подлинным владельцем закрытого ключа. Степень достоверности факта установления подлинности зависит

от надежности хранения закрытого ключа и надежности источника поставки открытых ключей пользователей.

Процедура, позволяющая каждому пользователю устанавливать однозначное и достоверное соответствие между открытым ключом и его владельцем, обеспечивается механизмом сертификации открытых ключей.

Для того чтобы пользователь мог доверять процессу аутентификации, он должен извлекать открытый ключ другого пользователя из надежного источника, которому он доверяет. Таким источником в X.509 является *Удостоверяющий центр* (Certification authority), обеспечивающий формирование сертификатов.

Формат сертификатов, определенный требованиями X.509, включает следующую информацию: номер версии сертификата, серийный номер сертификата, идентификатор алгоритма, используемого для подписи УЦ, сведения об издателе сертификата, период действия сертификата, состоящий из дат начала и конца периода, сведения о владельце сертификата, информацию об открытом ключе пользователя — идентификатор алгоритма и собственно открытый ключ, дополнительные атрибуты (расширения), определяемые требованиями использования сертификата в системе, подпись *Удостоверяющего центра*.

Сертификаты имеют период действия, однако любой сертификат может быть выведен из обращения (аннулирован/отозван) или приостановлено его действие до истечения определенного периода, если закрытый ключ пользователя скомпрометирован, владелец сертификата больше не обслуживается УЦ, изменились атрибуты владельца сертификата.

Удостоверяющий центр для информирования пользователей об отозванных сертификатах поддерживает список отозванных сертификатов (COC).

Список отозванных сертификатов представляет собой подписанный *Удостоверяющим центром* блок информации, содержащий:

— идентификатор алгоритма подписи;

— уникальное имя УЦ;

— период действия (даты начала и конца периода);

— список, представляющий собой последовательность пар: серийный номер сертификата, дата отзыва.

Удостоверяющий центр InfoTrust издает сертификаты пользователей в электронной форме формата X.509 версии 3 и список отозванных сертификатов (COC) в электронной форме формата X.509 версии 2.

Криптографические алгоритмы, используемые Удостоверяющим центром InfoTrust — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012, ГОСТ 28147-89. Указанные алгоритмы реализуются сертифицированным в установленном порядке средствами криптографической защиты информации.

Дополнительные атрибуты сертификата содержат в соответствии с требованиями законодательства сведения об ограничениях и приложениях, построенных на основе технологии Инфраструктуры открытых ключей, и при которых электронный документ будет иметь юридическое значение. Указанные сведения представляются в виде набора объектных идентификаторов (OID), определяющих отношения, при осуществлении которых электронный документ с подписью, сформированный с закрытым ключом, соответствующим данному сертификату, будет иметь юридическое значение. В сертификаты включаются зарегистрированные в установленном порядке объектные идентификаторы сфер применения и профилей сертификатов, определенные в Перечне объектных идентификаторов ООО НПП «Ижинформпроект» (OID index) (OID 1.2.643.3.34.1.6).

Удостоверяющий центр выпускает сертификаты в соответствии Правилами применения сертификатов Удостоверяющего центра InfoTrust (Certificates Policy — CP), которые регламентируют применение сертификата для разрешенных приложений и систем с установленными требованиями безопасности (OID 1.2.643.3.34.1.2), в порядке, определенном Регламентом Удостоверяющего центра InfoTrust (OID 1.2.643.3.34.1.1).

Пользователь прикладной информационно-телекоммуникационной системы (уполномоченный представитель Абонента Системы) получает услуги

Удостоверяющего центра InfoTrust по изготовлению сертификатов и дополнительные услуги, связанные с управлением сертификатами ключей подписи.

Стоимость услуг, оказываемых Удостоверяющим центром, представлена в Прейскуранте (Price Current) (OID 1.2.643.3.34.1.5).

Сертификаты могут применяться в стандартных приложениях Инфраструктуры открытых ключей с любой комбинацией следующих областей применения:

— защита соединений в Интернете с использованием протокола TLS/SSL — проверка подлинности сервера и клиента;

— защищенная электронная почта с использованием стандарта S/MIME (подпись для аутентификации отправителя и гарантии подлинности и целостности сообщения и шифрование данных);

— компоненты с подписью (подпись электронных документов и кода программ);

— формирование штампов времени и применение служб актуального статуса сертификатов для реализации форматов усовершенствованной электронной подписи (CAdES/XAdES/PAdES);

и в защищенных информационно-телекоммуникационных системах построенных с использованием этих стандартных приложений.

Условия и порядок взаимодействия абонентов и использования при этом сертификатов, изготовленных *Удостоверяющим центром* InfoTrust, в информационно-телекоммуникационных системах, основанных на технологии Инфраструктуры открытых ключей, определяется нормативными документами (договоры, положения, соглашения, регламенты и т.п.) этих систем.

Условия и порядок взаимодействия абонентов и использования при этом сертификатов, выпущенных Удостоверяющим центром InfoTrust, в информационных системах общего пользования, определяются нормативными документами Российской Федерации.

Порядок регистрации пользователей, генерации ключевых документов, формирования запросов на сертификат, изготовления сертификата, отзыва сертификата и перечень необходимых документов, используемых при этом, определен Регламентом Удостоверяющего центра InfoTrust (OID 1.2.643.3.34.1.1).

Пользователи Удостоверяющего центра могут по запросу получить сертификаты других владельцев пользователей УЦ.

Удостоверяющий центр несет ответственность за убытки при использовании закрытого ключа подписи и сертификата пользователя, только в случае если данные убытки возникли при компрометации закрытого ключа уполномоченного лица Удостоверяющего центра, либо вследствие несоответствий сведений в сертификате сведениям, указанным в заявлении пользователя.

Сертификаты уполномоченного лица Удостоверяющего центра InfoTrust, действующие списки отозванных сертификатов, Прейскурант и необходимые нормативные документы, касающиеся функционирования Удостоверяющего центра InfoTrust и использования изготовленных сертификатов в прикладных системах опубликованы на официальном сайте Удостоверяющего центра по адресу http://www.infotrust.ru.

