Toyota
Financial Services

РЕГЛАМЕНТ
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА
АКЦИОНЕРНОГО ОБЩЕСТВА «ТОЙОТА БАНК»

Москва 2021

АО «Тойота Банк»
ул. Отрадная, 2Б, стр. 1
127273, Россия, г. Москва
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

СОДЕРЖАНИЕ

АО «Тойота Банк»
ул. Отрадная, 2Б, стр. 1
127273, Россия, г. Москва
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Сертификат ключа проверки электронной подписи (Сертификат) – электронный документ или документ на бумажном носителе, выданный Удостоверяющим центром либо доверенным лицом Удостоверяющего центра и подтверждающий принадлежность Ключа проверки электронной подписи Владельцу сертификата.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания Электронной подписи.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с Ключом электронной подписи и предназначенная для проверки подлинности Электронной подписи (проверка Электронной подписи).

Криптоключи – совместно именуемые Ключ электронной подписи и Ключ проверки электронной подписи.

Удостоверяющий центр АО «Тойота Банк» – совокупность программно-аппаратных средств, организационно-технических мероприятий и ответственных лиц АО «Тойота Банк», осуществляющих функции по созданию и выдаче Сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные действующим законодательством Российской Федерации.

Клиент – юридическое лицо, осуществляющее обмен информацией в электронной форме с АО «Тойота Банк» с использованием услуг Удостоверяющего центра.

Заявитель – юридическое или физическое лицо, обратившееся с запросом в Удостоверяющий центр на создание Сертификата ключа проверки электронной подписи.

Владелец сертификата – юридическое или физическое лицо, которому в установленном действующим законодательством Российской Федерации порядке выдан Сертификат ключа проверки электронной подписи.

Пользователь сертификата – физическое лицо, являющееся Владельцем сертификата, или физическое лицо, действующие от имени юридического лица, являющегося Владельцем сертификата.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание Электронной подписи, проверка Электронной подписи, создание Криптоключей.

Стороны – Удостоверяющий центр и Клиенты; Сторона означает любая из Сторон.

АО «Тойота Банк»
ул. Отрадная, 2Б, стр. 1
127273, Россия, г. Москва
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

1. ВВЕДЕНИЕ

1.1. Общие положения

Настоящий регламент Удостоверяющего центра Акционерного общества «Тойота Банк» (далее – Регламент) устанавливает порядок, правила и особенности осуществления Удостоверяющим центром Акционерного общества «Тойота Банк» (далее – Удостоверяющий центр) функций по созданию и выдаче Сертификатов ключей проверки электронных подписей (далее – Сертификатов), а также иных функций, предусмотренных действующим законодательством Российской Федерации в области использования Электронных подписей, и регулирует права и обязанности Сторон при электронном взаимодействии с использованием Электронных подписей.

Регламент разработан на основании и в соответствии с положениями действующих нормативно-правовых актов, методических документов уполномоченных федеральных органов исполнительной власти Российской Федерации и организационно-распорядительных документов Акционерного общества «Тойота Банк» (далее – АО «Тойота Банк») в области использования Электронных подписей, а также лучших практик в области инфраструктур открытых ключей (*Public Key Infrastructure*).

Все приложения, изменения, дополнения к Регламенту являются его составной и неотъемлемой частью.

Регламент утвержден президентом АО «Тойота Банк» приказом №043-01/21 от 17 июня 2021 года.

Срок действия Регламента не ограничен.

Внесение изменений и/или дополнений в Регламент, в том числе в приложения к нему, производится АО «Тойота Банк» в одностороннем порядке.

Официальное уведомление о внесении изменений и/или дополнений в Регламент производится АО «Тойота Банк» путем публикации соответствующей информации на web-сайте АО «Тойота Банк» по URL-адресу: *www.toyota-bank.ru*.

Все изменения и/или дополнения, вносимые АО «Тойота Банк» в Регламент и не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными для Сторон по истечении 10 (Десяти) рабочих дней с момента официального уведомления.

Любые изменения и/или дополнения в Регламент с момента вступления в силу равно распространяются на все Стороны, добровольно признавшие его, в том числе признавшие его ранее момента вступления изменений и/или дополнений в силу.

Официальное уведомление о прекращении действия Регламента осуществляется путем публикации соответствующей информации на web-сайте АО «Тойота Банк» по URL-адресу: *www.toyota-bank.ru*, не менее чем за 1 (Один) месяц до прекращения действия Регламента.

1.2. Идентификация Регламента

Наименование документа: «Регламент удостоверяющего центра Акционерного общества «Тойота Банк».

АО «Тойота Банк»
ул. Отрадная, 2Б, стр. 1
127273, Россия, г. Москва
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

Регламент доступен:

- в виде электронного документа, подписанного Электронной подписью уполномоченного лица Удостоверяющего центра, по URL-адресу: *www.toyota-bank.ru*;
- в бумажной форме в офисе АО «Тойота Банк» по адресу: 127273, Россия, г. Москва, ул. Отрадная, 2Б, строение 1.

Регламент не содержит информацию ограниченного доступа.

1.3. Область применения Регламента

Действие Регламента распространяется на все процессы функционирования Удостоверяющего центра и организационно-технические мероприятия, направленные на обеспечение его функционирования.

Регламент налагает обязательства на все вовлеченные в электронное взаимодействие с использованием Электронных подписей Стороны, а также служит средством официального уведомления и информирования всех Сторон.

Применение Регламента основано на его добровольном признании взаимодействующими Сторонами. Добровольное признание Регламента Клиентом является основанием для заключения с ним договора на соответствующий вид обслуживания и присоединения к соглашению об электронном взаимодействии с использованием Электронных подписей (далее – Соглашение).

Выпущенные Удостоверяющим центром Сертификаты могут применяться в любых информационных системах, требующих выполнения операций с использованием Электронной подписи, Сертификата и/или Криптоключей.

1.4. Контактная информация

Владелец Удостоверяющего центра – АО «Тойота Банк».

Полное наименование: Акционерное общество «Тойота Банк».

Юридический адрес: 127273, Россия, г. Москва, ул. Отрадная, 2Б, строение 1.

Фактический адрес: 127273, Россия, г. Москва, ул. Отрадная, 2Б, строение 1.

ИНН 7750004136, КПП 771501001, Кор./счет 30101810600000000630 в Отделение 3 ГУ Банка России по ЦФО г. Москва, БИК 044525630.

Уполномоченное лицо Удостоверяющего центра – Кузин А.Ю.

Контактный телефон: +7 (495) 644 1000.

АО «Тойота Банк» осуществляет свою деятельность на основании лицензий ФСБ России на деятельность в отношении шифровальных (криптографических) средств № 0012043 от 6 октября 2015 года, выданной Центром по лицензированию, сертификации и защите государственной тайны ФСБ России.

Toyota Financial Services

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Функции, обязанности и права Удостоверяющего центра

2.1.1. Функции (услуги) Удостоверяющего центра

Удостоверяющий центр обеспечивает применение усиленной неквалифицированной Электронной подписи в соответствии с положениями Федерального закона Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Срок действия Ключа электронной подписи, соответствующего корневому Сертификату Удостоверяющего центра, составляет 5 лет.

Начало периода действия Ключа электронной подписи, соответствующего корневому Сертификату Удостоверяющего центра, исчисляется с даты и времени начала действия соответствующего Сертификата.

Срок действия корневого Сертификата Удостоверяющего центра составляет 10 лет.

Информация в электронной форме, подписанная усиленной неквалифицированной Электронной подписью с использованием Сертификатов, созданных Удостоверяющим центром, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных Соглашением.

Удостоверяющий центр реализует следующие функции (предоставляет услуги):

- создает Сертификаты и выдает их лицам, обратившимся за их получением (Заявителям);
- аннулирует Сертификаты, выданные Заявителям;
- ведет реестр выданных и аннулированных им Сертификатов (далее – Реестр сертификатов и Список аннулированных сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных им Сертификатах, и информацию о датах прекращения действия или аннулирования Сертификатов и об основаниях таких прекращений или аннулирований;
- выдает по обращению Заявителя Средства электронной подписи, содержащие Криптоключи (в том числе созданные Удостоверяющим центром) или обеспечивающие возможность создания Криптоключей;
- предоставляет сведения об аннулированных им и приостановленных Сертификатах;
- создает по обращениям Заявителей Криптоключи;
- проверяет уникальность Ключей проверки электронных подписей в Реестре сертификатов;
- осуществляет проверку Электронных подписей по обращениям Пользователей сертификатов.

2.1.2. Обязанности Удостоверяющего центра

Удостоверяющий центр обязуется:

- своевременно информировать в письменной форме Клиентов об условиях и о порядке использования Электронных подписей и Средств электронной подписи, о рисках, связанных с использованием Электронных подписей, и о мерах, необходимых для обеспечения безопасности Электронных подписей и их проверки;

- установить сроки действия и область применения Сертификатов;
- установить порядок ведения Реестра сертификатов и порядок доступа к нему;
- обеспечить актуальность информации, содержащейся в Реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- предоставить безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к Реестру сертификатов информацию, содержащуюся в Реестре сертификатов, в том числе информацию об аннулировании Сертификата, а также корневом Сертификате Удостоверяющего центра в электронной форме;
- обеспечить конфиденциальность созданных Удостоверяющим центром Ключей электронных подписей.

Для обеспечения процессов функционирования Удостоверяющего центра в АО «Тойота Банк» назначены следующие лица:

- уполномоченное лицо Удостоверяющего центра;
- лицо, ответственное за техническое обеспечение Удостоверяющего центра;
- лицо, ответственное за технологическое обеспечение Удостоверяющего центра;
- лицо, ответственное за обеспечение информационной безопасности Удостоверяющего центра.

Деятельность Удостоверяющего центра может быть прекращена в порядке, установленном действующим законодательством Российской Федерации.

2.1.3. Права Удостоверяющего центра

Удостоверяющий центр вправе:

- отказать в изготовлении Криптоключей Заявителям, подавшим заявление на изготовление Криптоключей, с указанием причин отказа;
- отказать в изготовлении Сертификата Заявителям, подавшим заявление (запрос) на изготовление Сертификата, с указанием причин отказа;
- отказать в аннулировании (отзыве) Сертификата Пользователю сертификата, подавшему заявление на аннулирование (отзыв) Сертификата, в случае если истек установленный срок действия Ключа электронной подписи, соответствующий Ключу проверки электронной подписи;
- отказать в приостановлении или возобновлении действия Сертификата Пользователю сертификата, подавшему заявление на приостановлении или возобновлении действия Сертификата, в случае если истек установленный срок действия Ключа электронной подписи, соответствующий Ключу проверки электронной подписи;
- аннулировать (отозвать) Сертификат в случае установленного факта компрометации соответствующего Ключа электронной подписи, с уведомлением Пользователя аннулированного (отозванного) Сертификата и указанием причин;
- приостановить действие Сертификата, с уведомлением Пользователя приостановленного Сертификата и указанием причин;

- отказать Пользователю сертификата в проверке Электронных подписей в электронном документе, с указанием причин отказа.

2.2. Обязанности и права Клиентов Удостоверяющего центра

2.2.1. Обязанности Клиентов

Клиенты обязуются:

- ознакомиться с положениями Регламента, Соглашения и эксплуатационной документацией на используемые Средства электронной подписи, а также не реже 1 (Одного) раза в квартал обращаться по URL-адресу: *www.toyota-bank.ru*, за сведениями об изменениях и/или дополнениях к данным документам;
- своевременно предоставить полную и достоверную информацию, необходимую для создания Сертификатов;
- обеспечить условия для применения Сертификатов и Средств электронной подписи;
- соблюдать порядок, правила и ограничения на использование Сертификатов и Средств электронной подписи;
- обеспечить конфиденциальность Ключей электронных подписей;
- уведомить Удостоверяющий центр о нарушении конфиденциальности Ключа электронной подписи в течение не более чем 1 (Одного) рабочего дня со дня получения информации о таком нарушении;
- не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

2.2.2. Права Клиентов

Клиенты вправе:

- получить Список аннулированных сертификатов, изготовленный Удостоверяющим центром;
- получить корневой Сертификат Удостоверяющего центра;
- получить копию Сертификата для соответствующего Владельца сертификата в электронной форме, находящегося в Реестре сертификатов Удостоверяющего центра;
- применять корневой Сертификат Удостоверяющего центра для проверки Электронной подписи в Сертификатах, изготовленных Удостоверяющим центром;
- применять Список аннулированных сертификатов, изготовленный Удостоверяющим центром, для проверки статуса Сертификатов.
- обратиться в Удостоверяющий центр за подтверждением подлинности Электронных подписей в документах, представленных в электронной форме;
- обратиться в Удостоверяющий центр на предмет получения (приобретения) Средств электронной подписи;
- обратиться в Удостоверяющий центр для изготовления Криптоключей;

- обратиться в Удостоверяющий центр для аннулирования (отзыва) Сертификатов для соответствующих Владельцев сертификата в течение срока их действия;
- обратиться в Удостоверяющий центр для приостановления действия Сертификатов для соответствующих Владельцев сертификата в течение срока их действия;
- обратиться в Удостоверяющий центр для возобновления действия Сертификатов для соответствующих Владельцев сертификата в течение срока их действия (в случае если их действие было приостановлено).

2.3. Ответственность Сторон

За невыполнение или ненадлежащее выполнение положений Регламента Стороны несут материальную ответственность в размере доказанного ущерба, причиненного Стороне вследствие соответствующих действий, в соответствии с действующим законодательством Российской Федерации.

Стороны не несут ответственность за неисполнение или ненадлежащее исполнение обязательств по Регламенту вследствие возникновения чрезвычайных ситуаций природного, техногенного характера или вследствие действий государства (форс-мажор). В случае возникновения подобных ситуаций, они должны быть документально подтверждены Сторонами.

Удостоверяющий центр не несет ответственности в случае нарушения Клиентами положений Регламента, Соглашения и/или эксплуатационной документацией на используемые Средства электронной подписи.

2.4. Разрешение споров между Сторонами

При рассмотрении спорных вопросов, связанных с настоящим Регламентом, Стороны руководствуются действующим законодательством Российской Федерации.

Спорные вопросы, связанные с настоящим Регламентом, решаются Сторонами в претензионном порядке.

Сторона, получившая претензию, обязана в течение 10 (Десяти) рабочих дней удовлетворить предъявленные требования или направить мотивированный отказ с приложением всех соответствующих документов.

В случае невозможности урегулировать спорные вопросы в претензионном порядке, Стороны решают их в Арбитражном суде города Москвы.

2.5. Вознаграждение Удостоверяющего центра

Удостоверяющий центр осуществляет свою деятельность на договорной основе.

Стоимость, сроки и порядок расчетов за оказанные Удостоверяющим центром услуги регулируются отдельными договорами с Клиентами.

Предоставление в электронной форме Сертификатов, находящихся в Реестре сертификатов, а также информации об их действии в виде Списков аннулированных сертификатов осуществляется Удостоверяющим центром безвозмездно.

Удостоверяющий центр аннулирует (отзывает) Сертификаты и осуществляет приостановление/возобновление их действия безвозмездно.

2.6. Публикация Реестра сертификатов и Списка аннулированных сертификатов

Реестр сертификатов и Список аннулированных сертификатов доступны в виде электронных документов на web-сайте АО «Тойота Банк» по URL-адресу: http://bank.toyota.ru/doc/AO_Toyota_Bank.crl

Список аннулированных сертификатов публикуется не реже 1 (Одного) раза в месяц. В случае аннулирования (отзыва) или приостановления/возобновления действия какого-либо из Сертификатов, Список аннулированных сертификатов публикуется немедленно.

Доступ к Реестру сертификатов и Списку аннулированных сертификатов регистрируется автоматизированными средствами web-сайта АО «Тойота Банк» в электронном журнале обращений.

Точка распространения Списков аннулированных сертификатов указывается в поле *CRL Distribution Point* Сертификата.

2.7. Аудит Удостоверяющего центра

С целью проверки соответствия деятельности Удостоверяющего центра требованиям Регламента, действующих нормативно-правовых актов, методических документов уполномоченных федеральных органов исполнительной власти Российской Федерации и организационно-распорядительных документов АО «Тойота Банк» в области использования Электронных подписей не реже 1 (Одного) раза в год проводится аудит.

Программа аудита, порядок проведения аудита, а также оценка аудиторов производится в соответствии с требованиями организационно-распорядительных документов АО «Тойота Банк» в области аудита (оценок соответствия).

Для проведения аудита могут привлекаться сторонние организации, обладающие соответствующей компетенцией и опытом оказания услуг в данной области.

Результаты аудита отражаются в соответствующих протоколах и используются для внесения предложений по изменению положений Регламента и других организационно-распорядительных документов АО «Тойота Банк» в области использования Электронных подписей с целью повышения качества услуг, предоставляемых Удостоверяющим центром.

2.8. Конфиденциальность

Следующие типы информации, возникающие в процессе функционирования Удостоверяющего центра и/или связанные с Удостоверяющим центром, являются информацией ограниченного доступа, и в отношении нее АО «Тойота Банк» принимает меры по обеспечению конфиденциальности:

- ключ электронной подписи уполномоченного лица Удостоверяющего центра и Ключ электронной подписи, соответствующий корневому Сертификату Удостоверяющего центра;
- пин-код для доступа к Ключу электронной подписи, записанному на специализированный съемный носитель информации (USB-ключ);

- персональная и корпоративная информация Клиентов, содержащаяся в Удостоверяющем центре, не подлежащая непосредственной рассылке в качестве части Сертификата и/или Списка аннулированных сертификатов;
- информация о конкретных средствах и способах защиты Удостоверяющего центра;
- информация, хранящаяся в электронных журналах аудита Удостоверяющего центра;
- отчетные материалы по выполненным проверкам деятельности Удостоверяющего центра в соответствии с пунктом 2.7 Регламента;
- Ключ электронной подписи Владельца сертификата (в случае изготовления его по запросу Заявителя).

Удостоверяющий центр не хранит, не архивирует и не депонирует Ключи электронной подписи, изготовленные по запросу Заявителей.

Информация, включаемая в Сертификаты, Реестр сертификатов и Списки аннулированных сертификатов, издаваемые Удостоверяющим центром, является общедоступной.

Удостоверяющий центр раскрывает информацию ограниченного доступа третьим лицам только в случаях, установленных действующим законодательством Российской Федерации.

Удостоверяющий центр обеспечивает актуальность информации, содержащейся в Реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий путем применения комплекса организационно-технических защитных мер в соответствии с разделом 5 Регламента.

АО «Тойота Банк»
ул. Отрадная, 2Б, стр. 1
127273, Россия, г. Москва
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

3.1. Идентификация и аутентификация Заявителей при регистрации

Под регистрацией Заявителей понимается добровольное признание ими Регламента и присоединение к Соглашению.

В случае необходимости Удостоверяющий центр проводит идентификацию и аутентификацию Заявителей (в зависимости от их типа):

- юридических лиц на основании свидетельства о постановке на налоговый учет и/или свидетельства о государственной регистрации;
- физических лиц на основании документов, удостоверяющих личность.

Имена, содержащиеся в Сертификатах (поле *Subject Name*), созданных Удостоверяющим центром, должны однозначно идентифицировать Владельца сертификата.

Создание Удостоверяющим центром анонимных Сертификатов не допускается.

Возможно существование нескольких Сертификатов с одинаковыми отличительными именами, однако Удостоверяющий центр гарантирует уникальность издаваемых Сертификатов (за счет использования поля *Certificate Serial Number*).

3.2. Идентификация и аутентификация Пользователей сертификатов в процессе жизненного цикла Сертификатов

Аутентификация и идентификация Пользователей сертификатов в процессе жизненного цикла Сертификатов осуществляется по:

- действительному Сертификату;
- заявлениям в формах, установленных Соглашением;
- документам, удостоверяющим личность.

АО «Тойота Банк»
ул. Отрадная, 2Б, стр. 1
127273, Россия, г. Москва
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

4. ПРОЦЕДУРЫ И МЕХАНИЗМЫ

4.1. Создание Криптоключей и запроса на создание Сертификата

Создание Криптоключей и запроса на создание Сертификата осуществляется Удостоверяющим центром на основании соответствующего запроса от Заявителя или Пользователя сертификата либо самостоятельно Заявителем или Пользователем сертификата.

В первом случае создание Криптоключей и запроса на создание Сертификата осуществляется лицом, ответственным за обеспечение информационной безопасности Удостоверяющего центра, на специализированном автоматизированном рабочем месте, аттестованном по требованиям безопасности информации с использованием Средств электронной подписи, обладающих действующим сертификатом соответствия требованиям по безопасности информации.

Изготовленные Криптоключи записываются на специализированный съемный носитель информации (USB-ключ) и защищаются пин-кодом на доступ.

Специализированный съемный носитель информации (USB-ключ) учитывается лицом, ответственным за обеспечение информационной безопасности Удостоверяющего центра, в журнале учета средств криптографической защиты информации и носителей ключевой информации, и передается Заявителю по акту, оформленному в бумажной форме и заверенному подписями ответственных лиц Удостоверяющего центра, либо после проставления Заявителем соответствующей отметки в журнале учета средств криптографической защиты информации и носителей ключевой информации, а запрос на создание Сертификата в электронной форме передается на обработку.

Во втором случае создание Криптоключей и запроса на создание Сертификата осуществляется Заявителем или Пользователем сертификата на своем рабочем месте с использованием Средств электронной подписи, обладающих действующим сертификатом соответствия требованиям по безопасности информации.

Изготовленные Криптоключи записываются на специализированный съемный носитель информации (USB-ключ) и защищаются пин-кодом на доступ, а запрос на создание Сертификата в электронной форме передается на обработку в Удостоверяющий центр.

4.2. Обработка запроса на создание Сертификата

Аутентификация и идентификация Заявителя осуществляется в соответствии с требованиями пункта 3.1 Регламента.

Аутентификация и идентификация Пользователя сертификата осуществляется в соответствии с требованиями пункта 3.2 Регламента.

Удостоверяющий центр может отклонить запрос на создание Сертификата в следующих случаях:

- запрос на создание Сертификата был передан способом, не соответствующим требованиям Регламента, Соглашения и/или в несоответствующем формате;
- данные, указанные в запросе на создание Сертификата, не соответствуют действительности;
- Заявитель нарушил каким-либо образом Соглашение;

- Заявитель не прошел процедуру аутентификации и идентификации в соответствии с требованиями раздела 3 Регламента.

Запрос на создание Сертификата принимается, если отсутствуют вышеперечисленные причины для его отклонения.

Удостоверяющий центр начинает обработку запроса на создание Сертификата с момента его получения. Запрос на создание Сертификата считается активным до момента его принятия или отклонения. После рассмотрения запроса на создание Сертификата Удостоверяющий центр должен вынести решение о его принятии или отклонении, в случае отклонения Заявитель или Пользователь сертификата должен быть проинформирован.

4.3. Создание Сертификата

Удостоверяющий центр издает Сертификаты по одобренным запросам на создание Сертификата в соответствии с требованиями настоящего Регламента и утвержденными внутренними процедурами Банка.

Сертификат издается в электронной форме с составлением акта признания Ключа проверки электронной подписи в бумажной форме.

Оповещением Заявителя считается получение им Сертификата в электронной форме и акта признания Ключа проверки электронной подписи в бумажной форме, заверенного ответственными лицами Удостоверяющего центра.

4.4. Признание Сертификата

После получения Сертификата и акта признания Ключа проверки электронной подписи Пользователь сертификата обязан провести проверку соответствия выданного Сертификата переданному им запросу на создание Сертификата. В случае обнаружения несоответствия Пользователь сертификата обязан немедленно уведомить об этом Удостоверяющий центр, после чего такой Сертификат отзывается и издается новый Сертификат в соответствии с требованиями пункта 4.3 Регламента.

Если несоответствий не выявлено, Пользователь сертификата должен заверить акт признания Ключа проверки электронной подписи, что считается признанием полученного им Сертификата.

После признания один экземпляр акта признания Ключа проверки электронной подписи остается у Владельца сертификата, а второй хранится в Удостоверяющем центре.

После того как Сертификат считается признанным Пользователем сертификата, Сертификат публикуется Удостоверяющим центром в Реестре сертификатов.

4.5. Использование Сертификата

Пользователь сертификата может использовать Ключ электронной подписи для создания Электронных подписей только после признания Сертификата в соответствии с требованиями пункта 4.4 Регламента.

Перед использованием Сертификата Пользователь сертификата обязан проверить статус используемого Сертификата и всех Сертификатов в цепочке сертификации, если хоть один

Toyota Financial Services

Сертификат в цепочке сертификации аннулирован или не удается проверить его статус, то использование Сертификата запрещается.

Хранение Сертификатов в Реестре сертификатов осуществляется Удостоверяющим центром в течение установленного срока действия данного Сертификата, а также после его истечения в течение срока исковой давности (не менее 3 (Трех) лет).

Срок действия Ключа электронной подписи Владельца сертификата, соответствующего Сертификату, составляет 1 (Один) год.

Начало периода действия Ключа электронной подписи Владельца сертификата исчисляется с даты и времени начала действия соответствующего Сертификата.

Срок действия Ключа проверки электронной подписи устанавливается равным сроку действия соответствующего Сертификата.

Срок действия Сертификата устанавливается Удостоверяющим центром в момент его изготовления.

4.6. Обновление Криптоключей

Обновление Криптоключей возможно в случае компрометации или подозрения в компрометации Ключа электронной подписи, а также в случае истечения срока действия Сертификата. Создание Криптоключей может совершаться как Пользователем сертификата, так и Удостоверяющим центром в соответствии с требованиями пункта 4.1 Регламента.

Запрос на создание Сертификата при обновлении Криптоключей подает Пользователь сертификата.

Одобрение запроса на создание Сертификата при обновлении Криптоключей осуществляется в соответствии с пунктом 4.1, а издание Сертификата в соответствии с пунктом 4.3 Регламента.

Оповещением считается получение Пользователем сертификата нового Сертификата.

Признание Сертификата осуществляется в соответствии с разделом 4.4 Регламента.

После того как обновленный Сертификат считается признанным Пользователем сертификата, он публикуется Удостоверяющим центром в Реестре сертификатов.

4.7. Изменение Сертификата

Изменением Сертификата является выдача нового Сертификата при необходимости изменения информации, включенной в существующий Сертификат. При этом старый Сертификат аннулируется.

Изменение Сертификата производится в случае, если информация, содержащаяся в Сертификате, становится не актуальной.

Запрос на изменение Сертификата может быть подан Пользователем сертификата.

Запрос на изменение Сертификата может быть подан следующими способами:

- в электронной форме в соответствии с требованиями Соглашения;
- в бумажной форме, заверенный подписью Пользователя сертификата.

Toyota Financial Services

Одобрение запроса на изменение Сертификата осуществляется в соответствии с пунктом 4.1, а издание Сертификата в соответствии с пунктом 4.3 Регламента.

Оповещением считается получение Пользователем сертификата нового Сертификата.

Признание Сертификата осуществляется в соответствии с разделом 4.4 Регламента.

После того как обновленный Сертификат считается признанным Пользователем сертификата, он публикуется Удостоверяющим центром в Реестре сертификатов.

4.8. Аннулирование Сертификата

По истечении срока действия Сертификата он автоматически считается аннулированным. Сертификат считается аннулированным, приостановленным или возобновленным с момента публикации Списка аннулированных сертификатов, содержащего информацию об изменении статуса данного Сертификата.

Сертификат должен быть аннулирован (отозван) при следующих обстоятельствах:

- при компрометации Ключа электронной подписи;
- при разрыве или несоблюдении Соглашения;
- при несоблюдении Пользователем сертификата требований Регламента, Соглашения и/или эксплуатационной документации на Средства электронной подписи;
- при прекращении деятельности Удостоверяющего центра;
- по запросу на отзыв Сертификата от Пользователя сертификата;
- в случае если Удостоверяющему центру стало известно о прекращении действия документа, на основании которого был создан Сертификат.

Запрос на аннулирование Сертификата может быть подан:

- Пользователем сертификата;
- лицом, ответственным за обеспечение информационной безопасности Удостоверяющего центра, если таковой располагает достоверной информацией, требующей аннулирования Сертификата.

Запрос на аннулирование Сертификата может быть подан следующими способами:

- в электронной форме в соответствии с требованиями Соглашения;
- в бумажной форме, заверенный подписью Пользователя сертификата.

Запрос на аннулирование Сертификата должен содержать следующую информацию:

- информацию, позволяющую однозначно идентифицировать Сертификат, например серийный номер;
- причину отзыва, например:
  - увольнение работника;
  - организационно-штатные изменения;
  - компрометация или подозрение на компрометацию;

- утеря или порча ключевого носителя;
- ошибка в Сертификате;

- дату и время отзыва, в случае необходимости немедленно аннулировать (отозвать) Сертификат – указать «немедленно».

После получения запроса на аннулирование Сертификата Удостоверяющий центр производит его проверку на соответствие вышеизложенным требованиям, и если таковая прошла успешно, то производит отзыв Сертификата с указанием соответствующей причины (поле *Reason Code* в Списке аннулированных сертификатов):

- 0 – не указана;
- 1 – компрометация Ключа электронной подписи;
- 2 – компрометация центра сертификации (Удостоверяющего центра);
- 3 – изменение принадлежности;
- 4 – замена Сертификата;
- 5 – прекращение деятельности Удостоверяющего центра,

если нет, то Удостоверяющий центр информирует об этом отправителя запроса в электронной форме в соответствии с требованиями Соглашения.

Запрос на аннулирование Сертификата рассматривается Удостоверяющим центром в течение 1 (Одного) рабочего дня с момента его получения.

После аннулирования Сертификата Пользователь такового уведомляется об этом, а Удостоверяющий центр публикует Список аннулированных сертификатов, содержащий информацию об аннулированном Сертификате.

Списки аннулированных сертификатов публикуется Удостоверяющим центром немедленно.

4.9. Приостановление действия Сертификата

Действие Сертификата должно быть приостановлено при следующих обстоятельствах:

- по запросу Пользователя сертификата;
- по решению Удостоверяющего центра.

Запрос на приостановление действия Сертификата может быть подан:

- Пользователем сертификата;
- лицом, ответственным за обеспечение информационной безопасности Удостоверяющего центра, если таковой располагает достоверной информацией, требующей приостановления действия Сертификата.

Запрос на приостановление действия Сертификата может быть подан следующими способами:

- в электронной или устной форме в соответствии с требованиями Соглашения;
- в бумажной форме, заверенный подписью Пользователя сертификата.

Запрос на приостановление действия Сертификата должен содержать следующую информацию:

- информацию, позволяющую однозначно идентифицировать Сертификат, например серийный номер;
- причину приостановления;
- дату и время приостановления, в случае необходимости немедленного приостановления действия Сертификата — указать «немедленно».

После получения запроса на приостановление действия Сертификата Удостоверяющий центр производит его проверку на соответствие вышеизложенным требованиям, и если таковая прошла успешно, то производит приостановление действия Сертификата, если нет, то Удостоверяющий центр информирует об этом отправителя запроса в электронной форме в соответствии с требованиями Соглашения.

Запрос на приостановление действия Сертификата рассматривается Удостоверяющим центром в течение 1 (Одного) рабочего дня с момента его получения.

После приостановления действия Сертификата Пользователь такового уведомляется об этом, а Список аннулированных сертификатов, не содержащий информацию о приостановлении Сертификата, публикуется Удостоверяющим центром немедленно.

4.10. Возобновление действия Сертификата

Действие Сертификата может быть возобновлено:

- по запросу Пользователя сертификата;
- по решению Удостоверяющего центра.

Запрос на возобновление действия Сертификата может быть подан:

- Пользователем сертификата;
- лицом, ответственным за обеспечение информационной безопасности Удостоверяющего центра, если таковой располагает достоверной информацией, требующей возобновления действия Сертификата.

Запрос на возобновление действия Сертификата может быть подан следующими способами:

- в электронной или устной форме в соответствии с требованиями Соглашения;
- в бумажной форме, заверенный подписью Пользователя сертификата.

Запрос на возобновление действия Сертификата должен содержать следующую информацию:

- информацию, позволяющую однозначно идентифицировать Сертификат, например серийный номер;
- дату и время возобновление, в случае необходимости немедленного возобновления действия Сертификата – указать «немедленно».

После получения запроса на возобновление действия Сертификата Удостоверяющий центр производит его проверку на соответствие вышеизложенным требованиям, и если таковая прошла успешно, то производит возобновление действия Сертификата, если нет, то Удостоверяющий

центр информирует об этом отправителя запроса в электронной форме в соответствии с требованиями Соглашения.

Запрос на возобновление действия Сертификата рассматривается Удостоверяющим центром в течение 1 (Одного) рабочего дня с момента его получения.

После возобновления действия Сертификата Пользователь такового уведомляется об этом, а Список аннулированных сертификатов, не содержащий информацию о приостановлении Сертификата, публикуется Удостоверяющим центром немедленно.

4.11. Проверка статуса Сертификатов (доступ к Реестру сертификатов)

Проверка статуса Сертификатов доступна Пользователям сертификатов, а также третьим лицам через Реестр сертификатов и Списки аннулированных сертификатов.

Сервис доступен круглосуточно через сеть Интернет (возможны технологические перерывы в работе).

Информация о размещении актуального Реестра сертификатов и Списка аннулированных сертификатов приведена в пункте 2.6 Регламента.

4.12. Проверка Электронной подписи

Запрос на подтверждение Электронной подписи в электронном документе может быть подан Пользователем сертификата.

Запрос на подтверждение Электронной подписи в электронном документе может быть подан следующими способами:

- в электронной форме в соответствии с требованиями Соглашения;
- в бумажной форме, заверенный подписью Пользователя сертификата.

Бремя доказательства достоверности даты и времени формирования Электронной подписи в электронном документе возлагается на Пользователя сертификата.

Обязательными приложениями к запросу на подтверждение Электронной подписи в электронном документе являются следующие файлы:

- электронный документ, содержащий Электронную подпись;
- файл, содержащий корневой Сертификат Удостоверяющего центра, являющегося издателем Сертификата, использованного для создания Электронной подписи в электронном документе;
- файл, содержащий Список аннулированных сертификатов, выпущенный Удостоверяющим центром, и использовавшийся Заявителем для проверки Электронной подписи электронного документа.

Срок рассмотрения запроса на подтверждение Электронной подписи в электронном документе составляет 5 (Пять) рабочих дней с момента его поступления в Удостоверяющий центр.

В случае отказа от подтверждения Электронной подписи в электронном документе обратившемуся Пользователю сертификата возвращается запрос с указанием причин отказа.

В случае принятия положительного решения, обратившемуся Пользователю сертификата предоставляется ответ в письменной форме, заверенный подписью уполномоченного лица Удостоверяющего центра, содержащий результат проверки соответствующим сертифицированным Средством электронной подписи с использованием Сертификата принадлежности Электронной подписи в электронном документе Владельцу сертификата и отсутствия искажений в подписанном данной Электронной подписью электронном документе.

4.13. Прекращение использования услуг

Клиент может отказаться от услуг Удостоверяющего центра следующим образом:

- отказавшись от обновления Сертификата по истечении срока его действия и расторгнув Соглашение;
- аннулировав (отозвав) Сертификат до истечения срока действия без выдачи нового и расторгнув Соглашение.

АО «Тойота Банк»
ул. Отрадная, 2Б, стр. 1
127273, Россия, г. Москва
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

5. МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

5.1. Объекты защиты

Защите силами АО «Тойота Банк» от несанкционированного доступа подлежат:

- аппаратно-программные средства Удостоверяющего центра;
- информация, содержащаяся в Реестре сертификатов и Списках аннулированных сертификатов;
- Ключи электронных подписей, соответствующие корневым Сертификатам Удостоверяющего центра;
- Ключи электронных подписей, выпущенные по запросу Заявителей.

5.2. Защита аппаратно-программных средств Удостоверяющего центра

Аппаратно-программные средства Удостоверяющего центра расположены на территории АО «Тойота Банк» в помещениях с ограниченным доступом, оборудованных системой контроля и управления доступом, а также системой видеонаблюдения.

Аппаратно-программные средства Удостоверяющего центра обеспечены средствами бесперебойного электропитания.

Электрические сети и электрооборудование, используемые в Удостоверяющем центре, отвечают требованиям действующих правил устройства электроустановок.

Помещения с аппаратно-программными средствами Удостоверяющего центра оборудованы средствами вентиляции и кондиционирования воздуха, а также средствами пожарной сигнализации и пожаротушения в соответствии с СН 512-78 «Инструкции по проектированию зданий и помещений для электронно-вычислительных машин».

5.3. Защита информации, содержащейся в Реестре сертификатов и Списках аннулированных сертификатов

Защита информации, содержащейся в Реестре сертификатов и Списках аннулированных сертификатов от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий достигается путем:

- ограничения доступа в помещения, где размещены аппаратные средства Удостоверяющего центра, а также хранятся носители защищаемой информации;
- идентификации, аутентификации и разграничения доступа пользователей и обслуживающего персонала к программным средствам Удостоверяющего центра и защищаемой информации;
- регистрации действий пользователей и обслуживающего персонала, контроля несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

- резервирования технических средств, дублирования массивов и носителей защищаемой информации;
- предотвращения внедрения вредоносных программ (программ-вирусов).

Мероприятия и средства защиты информации, используемые для защиты информационно-вычислительных ресурсов Удостоверяющего центра, обеспечивают нейтрализацию (парирование):

- угроз непосредственного доступа к защищаемой информации;
- угроз удаленного доступа к защищаемой информации.

Средства защиты информации обеспечивают:

- идентификацию и проверку подлинности обслуживающего персонала при обращении к защищаемой информации;
- регистрацию входа (выхода) обслуживающего персонала в операционные системы (из операционных систем) компонентов Удостоверяющего центра, а также попыток несанкционированного доступа к данным операционным системам;
- целостность своих компонентов;
- реализацию требований, предусмотренных комплексом документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» в части обеспечения безопасности персональных данных Владельцев сертификатов (физических лиц).

Средства защиты информации, используемые для защиты информационно-вычислительных ресурсов Удостоверяющего центра, обладают действующими сертификатами соответствия требованиям по безопасности информации.

5.4. Защита Ключей электронных подписей

Защита Ключей электронных подписей, соответствующих корневым Сертификатам Удостоверяющего центра, от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий достигается путем:

- ограничения доступа в помещения, где размещены Ключи электронных подписей, соответствующие корневым Сертификатам Удостоверяющего центра;
- использования съемных носителей информации (USB-ключей), обеспечивающих защищенное хранение данных;
- учет съемных носителей информации (USB-ключей), обеспечивающих защищенное хранение данных.

Средства электронной подписи, используемые для создания Ключей электронных подписей, обладают действующими сертификатами соответствия требованиям по безопасности информации.

Toyota Financial Services

5.5. Защита Ключей электронных подписей, выпущенных по запросу Заявителей

Защита Ключей электронных подписей, выпущенных по запросу Заявителей, от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий достигается путем:

- использования съемных носителей информации (USB-ключей), обеспечивающих защищенное хранение данных;
- раздельного предоставления Заявителю носителей информации и пин-кода для доступа к данному носителю.

Средства электронной подписи, используемые для создания Ключей электронных подписей, обладают действующими сертификатами соответствия требованиям по безопасности информации.

АО «Тойота Банк»
ул. Отрадная, 2Б, стр. 1
127273, Россия, г. Москва
+7 (495) 644 1000
www.toyota-bank.ru

Toyota Financial Services

6. СТРУКТУРЫ СЕРТИФИКАТОВ И СПИСКОВ АННУЛИРОВАННЫХ СЕРТИФИКАТОВ

6.1. Структура Сертификата

Удостоверяющий центр издает Сертификаты в электронной форме в соответствии с требованиями формата X.509 версии 3.

Базовые поля Сертификата приведены в таблице:

Наименование поля	Значение (комментарий)
Signature	Электронная подпись Удостоверяющего центра
Issuer Name	Идентифицирующие данные Удостоверяющего центра
Validity	Даты начала и окончания срока действия Сертификата
Subject Name	Идентифицирующие данные Владельца сертификата
Subject Public Key Information	Идентификатор алгоритма Средства электронной подписи, с которыми используется данный Ключ проверки электронной подписи, значение Ключа проверки электронной подписи
Version	Версия Сертификата формата X.509 – версия 3
Certificate Serial Number	Уникальный серийный (регистрационный) номер Сертификата в Реестре сертификатов Удостоверяющего центра

Дополнения Сертификата приведены в таблице:

Наименование поля	Значение (комментарий)
Authority Key Identifier	Идентификатор ключа Удостоверяющего центра
Subject Key Identifier	Идентификатор ключа Владельца сертификата
Extended Key Usage	Область (области) использования ключа, при которых электронный документ с Электронной подписью будет иметь юридическое значение (расширенное назначение ключа проверки электронной подписи)
CRL Distribution Point	Точка распространения Списка аннулированных сертификатов, изданных Удостоверяющим центром
Key Usage	Назначение ключа проверки Электронной подписи

Удостоверяющий центр использует следующие идентификаторы алгоритмов средства электронной подписи:

Наименование алгоритма	Идентификатор	Значение (комментарий)
ГОСТ Р 34.10-2012	1.2.643.7.1.1.1.1	Алгоритм Ключа проверки электронной подписи (длина ключей 256 бит)
	1.2.643.7.1.1.1.2	Алгоритм Ключа проверки электронной подписи (длина ключей 512 бит)

Наименование алгоритма	Идентификатор	Значение (комментарий)
ГОСТ Р 34.10-2012	1.2.643.7.1.1.3.2	Алгоритм Электронной подписи (длина ключей 256 бит)
	1.2.643.7.1.1.3.3	Алгоритм Электронной подписи (длина ключей 512 бит)
Диффи-Хеллмана	1.2.643.2.2.99	Алгоритм на базе экспоненциальной функции
Диффи-Хеллмана	1.2.643.2.2.98	Алгоритм на базе эллиптической кривой
ГОСТ Р 34.11-2012	1.2.643.7.1.1.2.2	Алгоритм хеширования (длина выхода 256 бит)
	1.2.643.7.1.1.2.3	Алгоритм хеширования (длина выхода 512 бит)
ГОСТ 28147-89	1.2.643.2.2.21	Алгоритм шифрования

В Сертификате поля идентификационных данных содержат атрибуты имени формата X.509.

Обязательными атрибутами поля идентификационных данных Владельца сертификата, являющегося физическим лицом, являются:

Наименование поля	Значение (комментарий)
Common Name	Фамилия, имя, отчество
Email	Адрес электронной почты
Country	RU

Обязательными атрибутами поля идентификационных данных Владельца сертификата, являющегося юридическим лицом, являются:

Наименование поля	Значение (комментарий)
Common Name	Полное наименование организации
Organization	Сокращенное наименование организации
Email	Адрес электронной почты
Country	RU
State	Субъект Российской Федерации, где зарегистрирована организация, которую представляет Владелец сертификата

6.2. Структура Списка аннулированных сертификатов

Удостоверяющий центр издает Списки аннулированных сертификатов в электронной форме в соответствии с требованиями формата X.509 версии 2.

Удостоверяющий центр использует следующие дополнения:

Наименование поля	Значение (комментарий)
Authority Key Identifier	Идентификатор ключа уполномоченного лица Удостоверяющего Центра
Reason Code	Код причины отзыва Сертификата
szOID_CERTSRV_CA_VERSION	Объектный идентификатор MS Certificate Server, определяющий версию службы сертификации MS CA

Toyota Financial Services

7. ЛИТЕРАТУРА

Перечень документов, использованных при разработке Регламента:

- Федеральный закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденная приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации № 152 от 13 июня 2001 г.
- ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».
- ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
- ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».
- Request for Comments: 2527 «Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework».
- Request for Comments: 3280 «Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile».
- СН 512-78 «Инструкции по проектированию зданий и помещений для электронно-вычислительных машин».

АО «Тойота Банк»
ул. Отрадная, 2Б, стр. 1
127273, Россия, г. Москва
+7 (495) 644 1000
www.toyota-bank.ru