

РУКОВОДСТВО УТВЕРЖДЕНО  
М. ЧАЙКИН  
ГЕНЕРАЛЬНЫЙ ДИРЕКТОР

ВСТУПАЕТ В СИЛУ С 01.03.2026

## **РЕГЛАМЕНТ**

предоставления услуг Оператора Удостоверяющего центра  
ООО «КРИПТО-ПРО» для Клиентов - юридических лиц

Редакция № 3.0

## 1. Сведения об Операторе Удостоверяющего центра

ИНГ БАНК (ЕВРАЗИЯ) АКЦИОНЕРНОЕ ОБЩЕСТВО, Генеральная лицензия № 2495, именуемое в дальнейшем «Оператор Удостоверяющего центра» («Оператор»), зарегистрированное на территории Российской Федерации.

### Реквизиты:

**Полное наименование:** ИНГ БАНК (ЕВРАЗИЯ) АКЦИОНЕРНОЕ ОБЩЕСТВО;

**Юридический адрес:** ул. Краснопролетарская, д. 36, Москва, 127473, Россия;

**Фактический адрес:** ул. Краснопролетарская, д. 36, Москва, 127473, Россия;

**Адрес для корреспонденции:** ул. Краснопролетарская, д. 36, Москва, 127473, Россия;

**Банковские реквизиты:**

БИК 044525222;

К/с 30101810500000000222;

**ИНН/КПП:** 7712014310/770701001;

**Контактные телефоны:**

тел. +7 (495)7555400.

## 2. Сведения об Удостоверяющем центре

Общество с ограниченной ответственностью «КРИПТО-ПРО», именуемое в дальнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Москва (Свидетельство о регистрации № 001.602.749 выдано 16.11.1999 г. Государственным учреждением Московской регистрационной палатой, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1037700085444 от 29.01.2003 г.).

Удостоверяющий центр в качестве профессионального участника рынка услуг по созданию и управлению неквалифицированными сертификатами ключей проверки электронной подписи осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий, опубликованных в сети Интернет по адресу: <https://www.cryptopro.ru/about/licenses>.

## 3. Термины и определения

*Электронный документ* – документ, информация в котором представлена в электронно-цифровой форме.

*Система «ИНГ Бизнес» (Система)* – корпоративная банковская система, предназначенная для подготовки и передачи Электронных документов, предусмотренных Условиями обслуживания расчетного обслуживания Клиентов – юридических лиц с использованием Системы «ИНГ Бизнес».

*Клиент* – юридическое лицо, присоединившееся к настоящему Регламенту путем предоставления надлежащим образом оформленного Подписного листа (Приложение №1).

*Средство электронной цифровой подписи* – средство криптографической защиты информации (СКЗИ) «РУТОКЕН ЭЦП 3.0», обеспечивающее реализацию следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание и хранение закрытых и открытых ключей электронных цифровых подписей.

*Электронная цифровая подпись (ЭЦП)* – усиленная неквалифицированная электронная подпись, являющаяся реквизитом электронного документа, предназначенным для защиты данного электронного документа от подделки, полученная в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

*Закрытый ключ электронной цифровой подписи (закрытый ключ подписи)* – ключ электронной подписи, являющийся уникальной последовательностью символов, известной владельцу сертификата ключа подписи и предназначенной для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Закрытый ключ электронной цифровой подписи действует на определенный момент времени (действующий закрытый ключ) если:

- наступил момент времени начала действия закрытого ключа;
- срок действия закрытого ключа не истек;
- сертификат открытого ключа подписи, соответствующий данному закрытому ключу не аннулирован (отозван) и действие его не приостановлено.

*Открытый ключ электронной цифровой подписи (открытый ключ подписи)* – ключ проверки электронной подписи, являющийся уникальной последовательностью символов, соответствующий закрытому ключу электронной цифровой подписи, предназначенной для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

*Сертификат ключа подписи (сертификат ключа электронной цифровой подписи, сертификат открытого ключа)* – неквалифицированный сертификат ключа проверки электронной подписи, являющийся электронным документом с электронной цифровой подписью уполномоченного лица Удостоверяющего центра, структура которого определяется настоящим Регламентом и который изготавливается Удостоверяющим центром для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Сертификат ключа подписи действует на определенный момент времени (действующий сертификат) если:

- наступил момент времени начала действия сертификата ключа подписи;
- срок действия сертификата ключа подписи не истек;
- сертификат ключа подписи не аннулирован (отозван) и действие его не приостановлено.

*Копия сертификата ключа подписи* – документ на бумажном носителе, содержащий информацию из сертификата ключа подписи и заверенный Оператором Удостоверяющего центра, либо Удостоверяющим центром.

*Список отозванных сертификатов (СОС)* – электронный документ с электронной цифровой подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были отозваны или действие которых было приостановлено.

*Владелец сертификата ключа подписи* – лицо, на имя которого Удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

*Удостоверяющий центр* – ООО «КРИПТО-ПРО», осуществляющее выполнение целевых функций удостоверяющего центра по изготовлению и управлению неквалифицированными сертификатами ключей проверки электронной подписи в соответствии с Федеральным законом «Об электронной подписи» в целях обеспечения применения участниками Информационной Системы неквалифицированной усиленной электронной подписи.

*Оператор Удостоверяющего центра (Оператор)* – ИНГ БАНК (ЕВРАЗИЯ) АКЦИОНЕРНОЕ ОБЩЕСТВО, наделенное Удостоверяющим центром правами по осуществлению действий по регистрации и управлению сертификатами ключей подписей Пользователей Удостоверяющего центра.

*Реестр Удостоверяющего центра* – набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий следующую информацию:

- реестр заявлений на регистрацию в Удостоверяющем центре;
- реестр зарегистрированных пользователей Удостоверяющего центра;
- реестр заявлений на изготовление сертификата ключа подписи;
- реестр заявлений на аннулирование (отзыв) сертификата ключа подписи;
- реестр сертификатов ключей подписи;
- реестр изготовленных списков отозванных сертификатов;

*Уполномоченное лицо Удостоверяющего центра* – физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов открытого ключа подписи и списков отозванных сертификатов.

*Пользователь Удостоверяющего центра (Пользователь УЦ)* – физическое лицо, зарегистрированное в Удостоверяющем центре и являющееся полномочным представителем Стороны, присоединившейся к Регламенту.

*Рабочий день Оператора Удостоверяющего центра (далее – рабочий день)* – промежуток времени с 09:00 по 17:30 (время Московское) каждого дня недели за исключением выходных и праздничных дней.

*Служба актуальных статусов сертификатов* – сервис Удостоверяющего центра, обеспечивающий информирование Пользователей о статусе сертификатов ключей подписей по протоколу OCSP (Online Certificate Status Protocol).

*Служба штампов времени* – сервис Удостоверяющего центра, обеспечивающий предоставление Пользователям Удостоверяющего центра штампов времени по протоколу TSP (Time-Stamp Protocol).

*Список отозванных сертификатов (COC)* – электронный документ с электронной цифровой подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были отозваны или действие которых было приостановлено.

*Штамп времени электронного документа (штамп времени)* – электронный документ, подписанный электронной цифровой подписью и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе.

*Cryptographic Message Syntax (CMS)* – стандарт криптографических сообщений, описанный в RFC 3852 и RFC 3369. Удостоверяющий центр использует в своей работе криптографические сообщения, соответствующие данному стандарту с учетом применения российских криптографических алгоритмов.

*Online Certificate Status Protocol (OCSP)* – протокол установления статуса сертификата открытого ключа, реализующий RFC 2560 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP».

*Public Key Cryptography Standards (PKCS)* – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. Удостоверяющий центр осуществляет свою работу в соответствии со следующим стандартом PKCS - PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат открытого ключа.

*Time-Stamp Protocol (TSP)* – протокол получения штампа времени, реализующий RFC 3161 «Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)».

## 4. Общие положения

### 4.1. Статус Регламента.

4.1.1. Настоящий Регламент предоставления услуг Оператора Удостоверяющего центра ООО «КРИПТО-ПРО» (далее – Регламент) является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

4.1.2. Настоящий Регламент является неотъемлемой частью Условий расчетного обслуживания Клиентов-юридических лиц с использованием Системы «ИНГ Бизнес».

Сторонами Регламента (далее – Стороны) являются ИНГ БАНК (ЕВРАЗИЯ) АКЦИОНЕРНОЕ ОБЩЕСТВО, выступающее Оператором Удостоверяющего центра, и Клиент, выступающий в качестве Стороны, присоединившейся к Регламенту. Любое заинтересованное лицо может ознакомиться с Регламентом, размещенным на сайте Оператора Удостоверяющего центра.

### 4.2. Присоединение к Регламенту.

4.2.1. Присоединение к Регламенту осуществляется путем подписания и предоставления Оператору Удостоверяющего центра Подписного листа к Регламенту по форме Приложения № 1 настоящего Регламента.

4.2.2. Факт присоединения лица к Регламенту является полным принятием условий настоящего Регламента и всех его приложений в редакции, действующей на момент подписания Подписного листа.

4.2.3. После присоединения к Регламенту в установленном порядке Стороны вступают в соответствующие договорные отношения на неопределённый срок.

4.2.4. Расторжение настоящего Регламента возможно только по соглашению Сторон. При этом Стороны до дня прекращения действия Регламента обязаны разрешить между собой все денежные и иные имущественные вопросы, связанные с настоящим Регламентом.

4.2.5. Прекращение действия Регламента не освобождает стороны от исполнения обязательств, возникших до указанного дня прекращения действия Регламента, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

### 4.3. Применение Регламента.

4.3.1. Стороны понимают термины, применяемые в настоящем Регламенте, строго в контексте общего смысла Регламента.

4.3.2. В случае противоречия и/или расхождения названия какого-либо раздела Регламента со смыслом какого-либо пункта в нем содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

4.3.3. В случае противоречия и/или расхождения положений какого-либо приложения к настоящему Регламенту с положениями собственно Регламента, Стороны считают доминирующим смысл и формулировки Регламента.

### 4.4. Изменение (дополнение) Регламента.

4.4.1. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Оператором в одностороннем порядке.

4.4.2. Уведомление присоединившейся стороны о внесении изменений (дополнений) в Регламент осуществляется Оператором направлением по Системе «ИНГ Бизнес» в адрес присоединившейся Стороны соответствующего информационного сообщения. Также такое уведомление может быть направлено заказным письмом по Почте России или курьерской службой.

4.4.3. Все изменения (дополнения), вносимые Оператором в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными для присоединившейся стороны по истечении 3 (трех) календарных дней с даты уведомления присоединившейся стороны о внесении указанных изменений (дополнений).

4.4.4. Все изменения (дополнения), вносимые Оператором в Регламент в связи с изменением действующего законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

4.4.5. Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу.

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

## **5. Предоставление информации**

5.1. Оператор вправе запросить у Стороны, присоединившейся к Регламенту, а присоединившаяся Сторона обязана предоставить Оператору документы, подтверждающие следующую информацию:

5.1.1. Наименование Организации и основной государственный регистрационный номер, идентификационный номер налогоплательщика.

5.1.2. нотариально заверенную копию Устава организации; нотариально заверенную копию учредительного договора (при наличии).

5.1.3. нотариально заверенную копию свидетельства о государственной регистрации.

5.1.4. копии протоколов, либо иных документов, о назначении уполномоченных лиц организации (в соответствии с учредительными документами организации) и/или надлежащим образом оформленные доверенности.

5.1.5. Сведения, необходимые для идентификации полномочного представителя Стороны, присоединившейся к Регламенту: фамилия, имя, отчество, номер паспорта, дата и орган выдачи, место регистрации.

## **6. Права и обязанности сторон**

6.1. Оператор обязан:

6.1.1. Обеспечить регистрацию Пользователей в Удостоверяющем центре по заявлениям на регистрацию в Удостоверяющем центре, в соответствии с порядком, определенным в настоящем Регламенте.

6.1.2. Занести регистрационную информацию Пользователей Удостоверяющего центра в Реестр Удостоверяющего центра.

6.1.3. Обеспечить изготовление сертификата ключа подписи зарегистрированного в Удостоверяющем центре лица по заявлениям на изготовление сертификата ключа подписи, в соответствии с порядком, определенным в настоящем Регламенте и официально уведомить об этом владельца изготовленного сертификата ключа подписи.

6.1.4. Аннулировать (отозвать) сертификат ключа подписи Пользователя Удостоверяющего центра по заявлению на аннулирование (отзыв) сертификата ключа подписи, в соответствии с порядком, определенным в настоящем Регламенте.

6.2. Сторона, присоединившаяся к Регламенту, обязана:

6.2.1. Известить Оператора об изменениях в наименовании Организации, государственного регистрационного номера, идентификационного номера налогоплательщика и по требованию Оператора предоставить документы, указанные в п. 5.1 настоящего Реглаamenta, в течение 5 (пяти) рабочих дней с момента регистрации изменений.

6.2.2. Аннулировать (отозвать) сертификат ключа подписи Пользователя Удостоверяющего центра в случае удаления прав Пользователя в Системе, в соответствии с порядком, определенным в настоящем Регламенте, не позднее 5 (пяти) рабочих дней с момента направления Оператору заявления по Приложению №1 к Условиям расчетного обслуживания Клиентов-юридических лиц с использованием Системы «ИНГ Бизнес».

6.2.3. Пользователь Удостоверяющего центра, являющийся полномочным представителем присоединившейся Стороны обязан:

6.2.3.1. Сформировать открытые и закрытые ключи подписи на своем рабочем месте только с использованием средства электронной цифровой подписи и программного обеспечения, указанных в Техническом регламенте Системы «ИНГ Бизнес», являющемся неотъемлемой частью Условий расчетного обслуживания Клиентов-юридических лиц с использованием Системы «ИНГ Бизнес».

6.2.3.2. Хранить в тайне личный закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

6.2.3.3. Применять для формирования электронной цифровой подписи только действующий личный закрытый ключ.

6.2.3.4. Не применять личный закрытый ключ, если ему стало известно, что этот ключ используется или использовался ранее другими лицами.

6.2.3.5. Немедленно обратиться к Оператору с заявлением на аннулирование действия сертификата ключа подписи в случае потери, раскрытия, искажения личного закрытого ключа, а также, в случае если Пользователю Удостоверяющего центра стало известно, что этот ключ используется или использовался ранее другими лицами.

6.2.3.6. Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на аннулирование (отзыв) которого подано на рассмотрение

Оператором, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) сертификата по момент времени официального уведомления об аннулировании (отзыве) сертификата.

6.2.3.7. Не использовать личный закрытый ключ до предоставления Оператору подписанной копии сертификата ключа подписи, соответствующего данному закрытому ключу.

6.3. Оператор имеет право:

6.3.1. Отказать в регистрации в Удостоверяющем центре уполномоченному представителю Стороны, присоединившейся к Регламенту, в случае ненадлежащего оформления необходимых регистрационных документов.

6.3.2. Отказать в изготовлении сертификата ключа подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления/не предоставления заявления на изготовление сертификата ключа подписи и/или согласия на обработку персональных данных.

6.3.3. Отказать в аннулировании (отзыве) сертификата ключа подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на аннулирование (отзыв) сертификата ключа подписи.

6.3.4. Отказать в аннулировании (отзыве) сертификата ключа подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату.

6.3.5. Аннулировать (отозвать) сертификат ключа подписи Пользователя Удостоверяющего центра самостоятельно в случае удаления Стороной, присоединившейся к Регламенту, прав Пользователя в Системе, в соответствии с порядком, определенным в настоящем Регламенте, в случае неполучения заявления на аннулирование (отзыв) сертификата ключа подписи.

6.4. Сторона, присоединившаяся к Регламенту, имеет право:

6.4.1. Получить сертификат ключа подписи уполномоченного лица Удостоверяющего центра.

6.4.2. Получить список отозванных сертификатов ключей подписи, изготовленный Удостоверяющим центром.

6.4.3. Применять сертификат ключа подписи уполномоченного лица Удостоверяющего центра для проверки электронной цифровой подписи уполномоченного лица Удостоверяющего центра в сертификатах ключей подписи, изготовленных Удостоверяющим центром.

6.4.4. Применять список отозванных сертификатов ключей подписи, изготовленный Удостоверяющим центром, для проверки статуса сертификатов ключей подписи, изготовленных Удостоверяющим центром.

6.4.5. Применять сертификат ключа подписи Пользователя Удостоверяющего центра для проверки электронной цифровой подписи электронных документов в соответствии со сведениями, указанными в сертификате ключа подписи.

6.4.6. Для хранения личного закрытого ключа применять средство криптографической защиты информации «РУТОКЕН ЭЦП 3.0», предоставленный Оператором.

6.4.7. Обратиться к Оператору для аннулирования (отзыва) сертификата ключа подписи в течение срока действия соответствующего закрытого ключа.

## **7. Ответственность сторон**

7.1. Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки, в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной Регламента своих обязательств.

7.2. Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется законодательством Российской Федерации.

## **8. Разрешение споров**

8.1. Сторонами в споре, в случае его возникновения, считаются Оператор и Сторона, присоединившаяся к Регламенту.

8.2. При рассмотрении спорных вопросов, связанных с настоящим Регламентом, Стороны будут руководствоваться действующим законодательством Российской Федерации.

8.3. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их путем переговоров.

8.4. Спорные вопросы между Сторонами, неурегулированные путем переговоров, решаются в Международном Коммерческом Арбитражном Суде при Торгово-Промышленной Палате Российской Федерации. Место рассмотрения споров - г. Москва. Язык арбитражного разбирательства – русский.

## **9. Порядок предоставления услуг Оператором Удостоверяющего центра**

9.1. Регистрация Пользователей Оператором Удостоверяющего центра

9.1.1. Оператор Удостоверяющего центра осуществляет регистрацию Пользователя в Удостоверяющем центре только в том случае, если Сторона, полномочным представителем которой является регистрирующееся лицо, присоединилась к настоящему Регламенту в соответствии с п. 4.2, предоставив Оператору Подписной лист к Регламенту по форме Приложения № 1 настоящего Регламента.

9.1.2. Регистрация Пользователя и изготовление сертификата

Пользователь производит установку и настройку своего рабочего места в соответствии с требованиями, указанными в Техническом регламенте Системы «ИНГ Бизнес» для клиентов-юридических лиц, являющимся неотъемлемой частью

Условий расчетного обслуживания Клиентов – юридических лиц с использованием Системы «ИНГ Бизнес».

Регистрация Пользователя и изготовление сертификата осуществляется Оператором Удостоверяющего центра на основании надлежащим образом оформленных и подписанных следующих документов, предоставленных Пользователем:

- Заявление на регистрацию Пользователя в Удостоверяющем центре ООО «КРИПТО-ПРО» и изготовление сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» (Приложение №2 настоящего Регламента);
- Согласие на обработку персональных данных (Приложение №2а), предоставляемое совместно с Заявлением на регистрацию Пользователя в Удостоверяющем центре ООО «КРИПТО-ПРО» и изготовление сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»;
- Акт признания открытого ключа ЭП (сертификата) для обмена сообщениями (Приложение №3).

Документы, указанные выше, за исключением Приложения № 2а, могут быть предоставлены, в том числе, по Системе «ИНГ Бизнес» и при этом должны быть подписаны ЭЦП единоличного исполнительного органа либо ЭЦП лица, уполномоченного Клиентом на заверение копий на основании доверенности, оформленной в соответствии с установленным порядком. В случае, если такая доверенность на уполномоченное лицо Клиента ранее Оператору не представлялась, она может быть направлена Оператору через Систему «ИНГ Бизнес», подписанная ЭЦП уполномоченного лица, одновременно с передаваемым Оператору пакетом Документов, указанных выше.

Согласие на обработку персональных данных (Приложение №2а) предоставляется при первичной регистрации Пользователя во всех случаях исключительно на бумажном носителе.

При этом при изготовлении сертификата первому Пользователю документы по форме Приложений № 1-3 настоящего Регламента, должны быть предоставлены в Банк только на бумажном носителе.

- В дополнение к вышеперечисленным документам Пользователь также должен сформировать в Системе и направить Оператору Запрос на сертификат открытого ключа. Порядок формирования данного Запроса описан в Руководстве по использованию Системы «ИНГ Бизнес» (Приложение 4 к Условиям расчетного обслуживания Клиентов – юридических лиц с использованием Системы «ИНГ Бизнес»).

Регистрация Пользователя и изготовление сертификата осуществляется Оператором Удостоверяющего центра при условии получения надлежаще оформленной доверенности на такого Пользователя при его подключении к Системе в

соответствии с Условиями расчетного обслуживания Клиентов – юридических лиц с использованием Системы «ИНГ Бизнес».

Оператор Удостоверяющего центра производит сравнение информации, указанной в вышеупомянутых документах на бумажном носителе и/или документах, полученных по Системе, с информацией, содержащейся в запросе на выпуск сертификата, поданном в электронной форме. В случае идентичности указанной идентификационной информации Пользователь регистрируется Оператором в Удостоверяющем центре и Пользователю выпускается сертификат открытого ключа Пользователя.

Оператор Удостоверяющего центра направляет Пользователю по электронной почте форму печати сертификата ключа подписи согласно Приложения №4 настоящего Регламента.

Пользователь распечатывает сертификат ключа подписи на бумажном носителе, подписывает собственноручно и передает Оператору Удостоверяющего центра. При необходимости наличия у Пользователя копии его сертификата на бумажном носителе, заверенном Оператором Удостоверяющего центра, Пользователь информирует Оператора Удостоверяющего центра об этом. Предоставление копии сертификата Пользователя на бумажном носителе, заверенного Оператором Удостоверяющего центра, осуществляется по согласованию с Оператором Удостоверяющего центра.

Регистрация Пользователя и изготовление сертификата, а также уведомление Пользователя о выпуске сертификата осуществляются не позднее 10 (десяти) рабочих дней, следующих за рабочим днем, в течение которого был получен Банком полный комплект документов (заявление на изготовление сертификата в электронном виде, а также заявления на бумажных носителях, необходимые для выпуска сертификата, указанные в настоящем пункте, включая согласие на обработку персональных данных).

Активация сертификата Пользователя производится только после предоставления Пользователем заверенной им копии сертификата Оператору Удостоверяющего центра. Оператор Удостоверяющего центра информирует Пользователя о возможности начала использования сертификата.

9.2. Изготовление и получение ключей подписи и сертификата ключа подписи  
Изготовление ключей подписи и сертификата открытого ключа Пользователя УЦ осуществляется при плановой и внеплановой смене закрытого ключа подписи Пользователя УЦ.

Продление срока действия (перевыпуск действующего ключа подписи) сертификата открытого ключа Пользователя УЦ осуществляется Оператором Удостоверяющего центра на основании сформированного в Системе Запроса на регенерацию сертификата, подписанное в Системе действующей на момент подписания подписью Пользователя. В дополнение к Запросу, сформированному в Системе, Пользователь должен предоставить Оператору УЦ подписанный «Акт признания открытого ключа

ЭП (сертификата) для обмена сообщениями» на бумажном носителе и/или по Системе.

Если на момент подписания Запроса на регенерацию сертификата подпись Пользователя уже недействительна, Пользователю следует руководствоваться порядком изготовления сертификата, установленным п. 9.1 настоящего Регламента.

В случае изменения данных, указанных в действующем сертификате ключа подписи Пользователя, такой сертификат должен быть перевыпущен в порядке изготовления сертификата, установленным п. 9.1 настоящего Регламента.

9.2.1. Изготовление и получение сертификата ключа подписи Значения поля Subject, содержащиеся в запросе на сертификат должны быть идентичны значениям этих полей в сертификате ключа подписи, соответствующего закрытому ключу Пользователя УЦ, которым сформирована электронная цифровая подпись на заявлении на изготовление сертификата ключа подписи Пользователя УЦ.

При принятии положительного решения Оператор Удостоверяющего центра принимает заявление на изготовление сертификата ключа подписи и осуществляет изготовление сертификата ключа подписи и направляет Пользователю по электронной почте копию сертификата ключа проверки электронной подписи Пользователя согласно Приложения №4.

Пользователь должен предоставить Оператору УЦ подписанную копию сертификата ключа проверки электронной подписи Пользователя на бумажном носителе и/или по Системе. Активация сертификата Пользователя производится только после предоставления Пользователем Оператору Удостоверяющего центра подписанной им копии сертификата ключа проверки электронной подписи Пользователя, предоставленного на бумажном носителе или по Системе.

9.3. Аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра

Для аннулирования (отзыва) сертификата ключа подписи Пользователь может предоставить заявление как в бумажной форме в соответствии с Приложением № 5 настоящего Регламента, так и в электронном виде через Систему.

Для предоставления заявления в электронном виде Пользователь УЦ формирует в Системе и направляет Оператору Удостоверяющего центра Запрос на отзыв сертификата обязательным указанием причины отзыва.

В случае компрометации или угрозы компрометации закрытого ключа Пользователь должен аннулировать сертификат ключа подписи.

После получения Запроса в Системе Оператор Удостоверяющего центра проверяет корректность электронной цифровой подписи заявления и устанавливает его автора, затем устанавливает – является ли автор заявления владельцем сертификата ключа подписи (отзываемого сертификата ключа подписи), серийный номер которого указан в запросе на отзыв сертификата ключа подписи.

Срок обработки заявления на аннулирование (отзыв) сертификата ключа подписи Оператором Удостоверяющего центра составляет 1 (один) рабочий день с даты получения Оператором такого заявления.

В случае отрицательного результата проведенных проверок, а также иных случаях, установленных настоящим Регламентом, Оператор Удостоверяющего центра отклоняет заявление на аннулирование (отзыв) сертификата ключа подписи.

При принятии положительного решения Оператор Удостоверяющего центра аннулирует (отзывает) сертификат ключа подписи. В этом случае такой сертификат ключа подписи становится недоступен к использованию Пользователем в Системе.

Временем аннулирования (отзыва) сертификата ключа подписи признается время издания Удостоверяющим центром Списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате, указанное в поле thisUpdate изданного Списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключа подписи в поле CRL Distribution Point.

## 10. Структура сертификатов ключей подписи и сроки действия ключевых документов

10.1. Структура сертификата ключа подписи уполномоченного лица Удостоверяющего центра

Название	Описание	Содержание
<b>Базовые поля сертификата</b>		
Version	Версия	V3
SerialNumber	Серийный номер	Уникальный серийный номер сертификата
SignatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	CommonName = УЦ КРИПТО-ПРО Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = <a href="mailto:cpca@cryptopro.ru">cpca@cryptopro.ru</a>
ValidityPeriod	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	CommonName = УЦ КРИПТО-ПРО Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = <a href="mailto:cpca@cryptopro.ru">cpca@cryptopro.ru</a>
PublicKey	Открытый ключ	Ключ проверки электронной подписи (алгоритм ГОСТ Р 34.10-2012)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
<b>Дополнения сертификата</b>		
Key Usage (critical)	Использование ключа	Неотрекаемость – невозможность осуществления отказа от совершенных действий; Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL)
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор ключа электронной подписи Удостоверяющего Центра, соответствующего данному сертификату
BasicConstraints	Основные ограничения	SubjectType (Тип владельца сертификата) =ЦС

		PathLengthConstraint (Ограничение на длину пути – ограничивает количество уровней иерархии при создании подчиненных Удостоверяющих центров)= Отсутствует
SzOID_CertSrv_CA_Version	Объектный идентификатор версии сертификата	Версия сертификата Удостоверяющего центра

## 10.2. Структура сертификата ключа подписи Пользователя Удостоверяющего центра

Название	Описание	Содержание
<b>Базовые поля сертификата</b>		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	CommonName = УЦ КРИПТО-ПРО Organization(Организация) = ООО КРИПТО-ПРО Locality(Город)= Москва Country(Страна)= RU Email(Электронная почта) = <a href="mailto:cpca@cryptopro.ru">cpca@cryptopro.ru</a>
ValidityPeriod	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	CommonName = Фамилия, Имя, Отчество или псевдоним OrganizationUnit = Подразделение Organization = Организация Title = Должность Locality = Город State = Субъект Федерации Country = Страна = RU Email = Электронная почта Компонента имени CN обязательна для заполнения, необходимость заполнения остальных значений определяется владельцем сертификата и Оператором Удостоверяющего центра. В поле Subject сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 3280
PublicKey	Открытый ключ	Ключ проверки электронной подписи (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
<b>Расширения сертификата</b>		
Key Usage (critical)	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Электронная подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшенный ключ	Набор областей использования ключей и сертификатов
Application Policy	Политика применения	Набор областей использования ключей и сертификатов
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор ключа электронной подписи Удостоверяющего Центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/hex.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, hex – шестнадцатеричное значение идентификатора ключа электронной подписи

		Удостоверяющего центра, с использованием которого издан сертификат и список отозванных сертификатов
Authority Information Access	Адрес Службы актуальных статусов сертификатов	URL адреса web-приложения Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OCSP
		В сертификат ключа проверки электронной подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280 и RFC 5280

### 10.3. Сроки действия ключевых документов

10.3.1. Срок действия закрытого ключа Уполномоченного лица Удостоверяющего центра составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности удостоверяющего центра, и для средства электронной цифровой подписи, с использованием которого данный закрытый ключ был сформирован.

Начало периода действия закрытого ключа уполномоченного лица Удостоверяющего центра исчисляется с даты и времени генерации закрытого ключа уполномоченного лица Удостоверяющего центра.

Срок действия сертификата ключа подписи Уполномоченного лица Удостоверяющего центра не превышает 30 (тридцать) лет. Время начала периода действия сертификата ключа подписи Уполномоченного лица Удостоверяющего центра и его окончания заносится в поля «notBefore» и «notAfter» поля «Validity Period» соответственно.

Срок действия закрытого ключа Пользователя Удостоверяющего центра составляет 1 (один) год. Пользователь самостоятельно осуществляет контроль за сроком действия выпущенного на свое имя закрытого ключа и в случае необходимости направляет запрос Оператору Удостоверяющего центра для его перевыпуска в соответствии с п. 9.2 настоящего Регламента.

Начало периода действия закрытого ключа Пользователя Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего сертификата ключа подписи.

Срок действия сертификата ключа подписи Пользователя Удостоверяющего центра не превышает 30 (тридцать) лет. Время начала периода действия сертификата ключа подписи Пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «notAfter» поля «Validity Period» соответственно.

Период времени действия закрытого ключа, соответствующего выданному сертификату ключа подписи Пользователя Удостоверяющего центра должен находиться в пределах периода времени, на который выдана Стороной, присоединившейся к Регламенту, соответствующая доверенность на совершение действий, определенных положениями настоящего Регламента для Пользователя Удостоверяющего центра. В случае если период действия закрытого ключа, соответствующего выданному сертификату ключа подписи Пользователя Удостоверяющего центра, менее периода действия доверенности на использование ключа таким Пользователем, оформленной и предоставленной Оператору в соответствии с Условиями расчетного обслуживания Клиентов – юридических лиц с использованием Системы «ИНГ Бизнес», Пользователь будет ограничен в использовании ЭЦП до момента продления его полномочий и предоставлении новой доверенности.

## 11. Дополнительные положения

11.1. Плановая смена ключей уполномоченного лица Удостоверяющего центра  
Плановая смена ключей (закрытого и соответствующего ему открытого ключа) Уполномоченного лица Удостоверяющего центра выполняется в период действия закрытого ключа Уполномоченного лица Удостоверяющего центра.

Процедура плановой смены ключей уполномоченного лица Удостоверяющего центра осуществляется в следующем порядке:

- Уполномоченное лицо Удостоверяющего центра генерирует новый закрытый и соответствующий ему открытый ключ;
- Уполномоченное лицо Удостоверяющего центра изготавливает новый сертификат ключа подписи уполномоченного лица Удостоверяющего центра

Старый закрытый ключ Уполномоченного лица Удостоверяющего центра используется в течение своего срока действия для формирования списков отозванных сертификатов, изданных Удостоверяющим центром в период действия старого закрытого ключа Уполномоченного лица Удостоверяющего центра.

По истечении одного года с момента проведения плановой смены ключей Уполномоченного лица Удостоверяющий центр изготавливает список отозванных сертификатов, соответствующий старому закрытому ключу, со сроком действия соответствующим сроку действия старого сертификата Уполномоченного лица Удостоверяющего центра (значение поля nextUpdate списка отозванных сертификатов совпадает со значением поля notAfter поля Validity сертификата ключа подписи Уполномоченного лица Удостоверяющего центра). Изданный список отозванных сертификатов публикуется Удостоверяющим центром, изготовление нового списка отозванных сертификатов, соответствующего старому закрытому ключу Уполномоченного лица Удостоверяющего центра, более не осуществляется.

11.2. Компрометация ключевых документов уполномоченного лица Удостоверяющего центра, внеплановая смена ключей уполномоченного лица Удостоверяющего центра.

В случае компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра сертификат Уполномоченного лица Удостоверяющего центра аннулируется (отзывается), Пользователи Удостоверяющего центра уведомляются об указанном факте путем рассылки соответствующего уведомления по электронной почте и публикации информации о компрометации на сайте Удостоверяющего центра. Все сертификаты, изданные с использованием скомпрометированного ключа Уполномоченного лица Удостоверяющего центра, считаются аннулированными.

После аннулирования сертификата Уполномоченного лица Удостоверяющего центра выполняется процедура внеплановой смены ключей Уполномоченного лица Удостоверяющего центра. Процедура внеплановой смены ключей Уполномоченного лица Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей Уполномоченного лица Удостоверяющего центра.

Все действовавшие на момент компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра сертификаты ключей подписей, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

### 11.3. Конфиденциальность информации

#### 11.3.1. Типы конфиденциальной информации.

11.3.1.1. Закрытый ключ, соответствующий сертификату ключа подписи, является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре. Оператор не осуществляет хранение закрытых ключей Пользователей Удостоверяющего центра.

11.3.1.2. Персональная и корпоративная информация о лицах, зарегистрированных в Удостоверяющем центре и содержащаяся в Реестре Удостоверяющего центра, не подлежащая непосредственной рассылке в качестве части сертификата ключа подписи, считается конфиденциальной.

11.3.2. Типы информации, не являющейся конфиденциальной.

11.3.2.1. Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

11.3.2.2. Информация, включаемая в сертификаты ключей подписи и списки отозванных сертификатов, издаваемые Удостоверяющим центром, не считается конфиденциальной.

11.3.2.3. Персональные данные, включаемые в сертификаты ключей подписей, издаваемые Удостоверяющим центром, относятся к персональным данным, предоставление которых разрешено Пользователем Оператору Удостоверяющего центра и Удостоверяющему центру для обеспечения изготовления и управления сертификатами.

11.3.2.4. Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.

#### 11.3.3. Исключительные полномочия Оператора и Удостоверяющего центра

11.3.3.1. Оператор и Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Российской Федерации.

### 11.4. Форс-мажор

11.4.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Регламенту, если это неисполнение явилось следствием форс-мажорных обстоятельств, возникших после присоединения к настоящему Регламенту.

11.4.2. Форс-мажорными обстоятельствами признаются чрезвычайные (т.е. находящиеся вне разумного контроля Сторон) и непредотвратимые при данных условиях обстоятельства включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по настоящему Регламенту.

11.4.3. В случае возникновения форс-мажорных обстоятельств срок исполнения Сторонами своих обязательств по настоящему Регламенту отодвигается соразмерно времени, в течение которого действуют такие обстоятельства.

11.4.4. Сторона, для которой создалась невозможность исполнения своих обязательств по настоящему Регламенту, должна в течение 2 (двух) рабочих дней

известить в письменной форме другую Сторону о наступлении, предполагаемом сроке действия и прекращении форс-мажорных обстоятельств.

11.4.5. Не извещение или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства.

11.4.6. В случае, если невозможность полного или частичного исполнения Сторонами какого-либо обязательства по настоящему Регламенту обусловлена действием форс-мажорных обстоятельств и существует свыше одного месяца, то каждая из Сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства и в этом случае ни одна из Сторон не вправе требовать возмещения возникших у нее убытков другой Стороной.

## **12. Список приложений**

12.1. Приложение №1. Подписной лист к Регламенту предоставления услуг Оператора Удостоверяющего центра ООО «КРИПТО-ПРО».

12.2. Приложение №2. Заявление на регистрацию Пользователя в Удостоверяющем центре ООО «КРИПТО-ПРО» и изготовление сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

12.3. Приложение №2а. Согласие на обработку персональных данных.

12.4. Приложение №3. Акт признания открытого ключа ЭП (сертификата) для обмена сообщениями (пример).

12.5. Приложение №4. Копия сертификата ключа проверки электронной подписи Пользователя (пример).

12.6. Приложение №5. Заявление на аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

**Приложение №1 к Регламенту предоставления услуг  
Оператора Удостоверяющего центра  
ООО «КРИПТО-ПРО»**

**Подписной лист к Регламенту  
предоставления услуг Оператора Удостоверяющего центра ООО  
«КРИПТО-ПРО»**

\_\_\_\_\_ (полное наименование организации, включая организационно-правовую форму)

зарегистрированное по адресу \_\_\_\_\_

\_\_\_\_\_ (местонахождения, указанное в учредительных документах)

в лице

\_\_\_\_\_,  
(должность)

\_\_\_\_\_,  
(фамилия, имя, отчество)

действующего на основании

\_\_\_\_\_  
в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяется к Регламенту предоставления услуг Оператора Удостоверяющего центра ООО «КРИПТО-ПРО» (далее Регламент), с настоящим Регламентом и приложениями к нему ознакомлен и является Стороной Регламента с момента подписания настоящего Подписного листа.

Подпись \_\_\_\_\_ / \_\_\_\_\_ /

М.П. (при наличии)

**Приложение №2 к Регламенту предоставления услуг  
Оператора Удостоверяющего центра  
ООО «КРИПТО-ПРО»**

**Заявление на регистрацию Пользователя в Удостоверяющем центре ООО  
«КРИПТО-ПРО» и изготовление сертификата ключа подписи Пользователя  
Удостоверяющего центра ООО «КРИПТО-ПРО»**

\_\_\_\_\_ (полное наименование организации, включая организационно-правовую форму)

в лице

\_\_\_\_\_ (должность)

\_\_\_\_\_ (фамилия, имя, отчество)

действующего на основании

просит зарегистрировать уполномоченного представителя (заполняется только при первичной регистрации уполномоченного представителя)

\_\_\_\_\_ (фамилия, имя, отчество)

в Реестре Удостоверяющего центра ООО «КРИПТО-ПРО» в качестве Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» для осуществления действий, установленных Регламентом предоставления услуг Оператора Удостоверяющего центра ООО «КРИПТО-ПРО».

просит изготовить сертификат ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

CommonName (CN): ФИО	
E-Mail (E): адрес электронной почты	
Organization (O): наименование организации	
Locality (L): город	
State (S): область	
Country (C): страна	

а также в соответствии с предоставленным Актом признания открытого ключа ЭП (сертификата) для обмена сообщениями (Приложение 3 настоящего Регламента), который необходимо приложить к настоящему Заявлению.

Подпись руководителя организации

\_\_\_\_\_ / \_\_\_\_\_ /

М.П. (при наличии)

**Приложение №2а к Регламенту предоставления услуг  
Оператора Удостоверяющего центра  
ООО «КРИПТО-ПРО»**

**Согласие на обработку персональных данных**

Я, субъект персональных данных,

\_\_\_\_\_  
ФИО субъекта персональных данных

основной документ,  
удостоверяющий личность:

\_\_\_\_\_  
наименование документа

\_\_\_\_\_  
серия

\_\_\_\_\_  
номер

\_\_\_\_\_  
дата выдачи, выдавший орган

зарегистрированный(ая) по адресу

\_\_\_\_\_  
адрес регистрации

свободно, своей волей и в своем интересе, в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», настоящим даю своё согласие **ИНГ БАНК (ЕВРАЗИЯ) АКЦИОНЕРНОЕ ОБЩЕСТВО** (далее – «Оператор»), расположенному по адресу: 127473, Россия, г. Москва, улица Краснопролетарская, 36, на обработку моих персональных данных.

<b>Цель:</b>	Ведение основной деятельности (осуществление банковских операций и иной деятельности, предусмотренной Уставом и лицензиями Банка, нормативными актами Банка России, действующим законодательством РФ), в том числе: <ul style="list-style-type: none"> <li>○ заключение договоров и обеспечение возможности предоставления услуг в соответствии с договором;</li> <li>○ предоставления доступа к системам дистанционного банковского обслуживания</li> </ul>
<b>Перечень персональных данных (ПДн)</b>	Ф.И.О. Название компании (места работы) Адрес электронной почты Адрес места жительства Номер телефона Данные документа, удостоверяющего личность Подпись
<b>Перечень действий с ПДн</b>	сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение
<b>Способы обработки</b>	в автоматизированной форме и без использования средств автоматизации
<b>Срок действия согласия</b>	на срок регистрации в Удостоверяющем центре ООО «КРИПТО-ПРО» и в течение 3 (трех) лет после прекращения регистрации в Удостоверяющем центре ООО «КРИПТО-ПРО»
<b>Поручение обработки ПДн</b>	Отсутствует
<b>Передача ПДн третьим лицам</b>	Оператор вправе привлекать третьих лиц, в том числе ООО «КРИПТО-ПРО» (ИНН: 7717107991) к обработке ПДн путем передачи третьим лицам ПДн. Привлечение третьих лиц к обработке ПДн может осуществляться только при условии обработки такими лицами ПДн в минимально необходимом составе и исключительно для достижения цели обработки ПДн, а также при условии обеспечения такими лицами конфиденциальности и безопасности ПДн при их обработке (в случае неисполнения третьими лицами данных условий указанные лица будут нести ответственность на основании своих договорных обязательств перед Оператором или в соответствии с положениями применимого законодательства о ПДн). С перечнем третьих лиц можно ознакомиться на сайте Оператора <a href="http://www.ing.ru">www.ing.ru</a>

Подписывая настоящее Согласие, я соглашаюсь с тем, что:

- Обработка ПДн (за исключением хранения) должна быть прекращена по достижению цели/целей обработки и прекращения обязательств по заключённым договорам и соглашениям, ПДн подлежат хранению в течение сроков, установленных законодательством Российской Федерации.
- Согласие может быть отозвано по письменному заявлению (отзыву) субъекта ПДн согласно п. 2 ст. 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» в любое время.

\_\_\_ . \_\_\_ . 20\_\_ г.

Дата

Подпись

Расшифровка подписи

**Приложение №3 к Регламенту предоставления услуг  
Оператора Удостоверяющего центра  
ООО «КРИПТО-ПРО»**

**Акт признания открытого ключа ЭП (сертификата)  
для обмена сообщениями  
(пример)**

**АКТ  
ПРИЗНАНИЯ ОТКРЫТОГО КЛЮЧА ЭП (СЕРТИФИКАТА)  
ДЛЯ ОБМЕНА СООБЩЕНИЯМИ**

Настоящим Актом признается ключ шифрования, принадлежащий уполномоченному представителю:

44	ФИО владельца сертификата:	543
45	Фамилия владельца сертификата:	
25	Имя и Отчество владельца сертификата:	
26	Должность владельца сертификата:	Главный бухгалтер
27	Адрес электронной почты владельца сертификата:	2132@mail.ru
28	Город:	454
29	Субъект Российской Федерации:	464
46	Организация:	ООО kn
30	ИНН физ.лица:	
30	ИНН:	66666666661
31	СНИЛС:	
32	ОГРН:	
33	ОГРНИП:	
34	Подразделение банка:	645
35	Номер запроса на сертификат:	5
37	Дата запроса:	11.02.2019 00:00:00
37	Дата начала срока действия сертификата:	11.02.2019 16:09:02
38	Дата окончания срока действия сертификата:	11.02.2020 16:19:02
39	Ключ ЭП создан с использованием СКЗИ:	КриптоПро
40	Идентификатор ключа:	DB03FDB51F7536700419026546F00-464EA638ED2
41	Местонахождение:	RU, 464, 454, 645
42	Хранилище ключевой информации:	Ir-0d34162b-1616-4041-8938-351dc00807fa
43	Момент генерации ключа:	11.02.2019 16:08:55
46	Тип идентификации при выдаче сертификата:	

Открытый ключ клиента:

```
04 81 80 FA 6B 9E 85 D3 3A 9E FA 73 0E 8C BD E8
01 3A 0E AC D3 8F 0F 33 99 BF A5 D3 FB 6B A2 A4
A0 7B AA C3 9D C4 CD 3B B6 99 F0 87 2B C3 84 34
94 2E C1 7A 92 B6 CD 6C 8D BF 66 6B CD 13 CB D5
AC F3 ED C3 29 43 9B 6D E8 15 28 12 82 14 04 89
55 3C AC F1 D1 91 07 55 BC 41 96 E9 73 DD B6 DF
16 7B FE 01 10 EC A2 DF B2 9B 8D 19 0B 9E 29 DB
31 44 B0 7F 17 C3 2E AD B0 EC 07 B7 41 19 F1 71
A6 2E CA
```

Достоверность приведенных данных подтверждаем

Владелец сертификата:

\_\_\_\_\_ /

От Банка

\_\_\_\_\_ /  
М.П.

Руководитель компании

(первая подпись согласно картонке образцов подписей)

\_\_\_\_\_ /

М.П.

**Приложение №4 к Регламенту предоставления услуг  
Оператора Удостоверяющего центра  
ООО «КРИПТО-ПРО»**

**Копия сертификата ключа проверки электронной подписи Пользователя  
(пример)**

**Сведения о сертификате:****Кому выдан:**

Фамилия Имя Отчество

**Кем выдан:**

УЦ КРИПТО-ПРО

Действителен с 31 января 2021 г. 21:30:28 UTC по 31 января 2036 г. 21:30:28 UTC

**Версия:** 3 (0x2)**Серийный номер:** 14F5 9CF2 0000 0000 003A**Алгоритм подписи:**

Название: ГОСТ Р 34.11/34.10-2012

Идентификатор: 1.2.643.2.2.3

Параметры: 0500

**Издатель сертификата:** CN = УЦ КРИПТО-ПРО, O = ООО КРИПТО-ПРО, L = Москва, C = RU, E = cpsa@cryptopro.ru**Срок действия:**

Действителен с: 15 мая 2023 г. 12:03:00 UTC

Действителен по: 15 мая 2024 г. 12:12:00 UTC

**Владелец сертификата:** CN = User1**Открытый ключ:**

Алгоритм открытого ключа:

Название: ГОСТ Р 34.10-2012

Идентификатор: 1.2.643.2.2.20

Параметры: 3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01

Значение: 0481 80A4 5A5B 0041 B273 F51E B062 322E CE6B 0480 5702 3FFF 5312 8FBA 1163 7381 5FED 445C 7DF9 F764 7822 99AA 3C3D 1E23 FE69  
B714 7062 36ED CB4A A834 7D5A 3525 BAC2 D80C 53DC 781B 4180 7CD3 ADD1 6D0E 00C9 9CA0 432F 595F 9CD3 12BE 69E6 A4D6 6133 227C DE1A 80F4  
D0F1 8337 843E CAD1 561F 793B CB05 EEBB EBD4 C23F E5EA ECD9 E6B5 A9**Расширения сертификата X.509**

1. Расширение 2.5.29.15 (критическое)

Название: Использование ключа

Значение: Цифровая подпись , Неотрекаемость , Шифрование ключей , Шифрование данных(F0)

2. Расширение 2.5.29.37

Название: Улучшенный ключ

Значение: Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)

3. Расширение 2.5.29.14

Название: Идентификатор ключа субъекта

Значение: 56BD CA83 3029 0673 CA83 3381 16D4 AF10 C3D6 9A75

4. Расширение 2.5.29.35

Название: Идентификатор ключа центра сертификатов

Значение: Идентификатор ключа=50AA 3E1E 4186 F8DC 3585 6E11 2C11 D9E3 0A91 7AD7 Поставщик сертификата: Адрес каталога: CN = УЦ КРИПТО-ПРО, O = ООО КРИПТО-ПРО, L = Москва, C = RU, E = cpsa@cryptopro.ru Серийный номер сертификата=29D1 B0C8 C311 ACAE 48DB AAB1 3687 CEFC

**Подпись Удостоверяющего центра:**

Алгоритм подписи:

Название: ГОСТ Р 34.11/34.10-2012

Идентификатор: 1.2.643.2.2.3

Параметры: 0500

Значение: 826C DDFB 331C 58C5 FD3D 9233 4A1D 2D7A B973 387C 8E8A DD3D 6FCE 0573 508A 3DC4 B29F 5961 FB6C D1EB 1B40 37C7 8473 5B0F FECA  
5E38 EA0C 3890 C77A C97E BD18 873A

Подпись уполномоченного лица УЦ: \_\_\_\_\_/\_\_\_\_\_

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Печать Удостоверяющего Центра

Подпись владельца сертификата: \_\_\_\_\_/\_\_\_\_\_

" \_\_\_\_ " \_\_\_\_\_ 20\_\_ г.

**Приложение №5 к Регламенту предоставления услуг  
Оператора Удостоверяющего центра  
ООО «КРИПТО-ПРО»**

**Заявление на аннулирование (отзыв) сертификата ключа подписи  
Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»**

\_\_\_\_\_ (полное наименование организации, включая организационно-правовую форму)

в лице

\_\_\_\_\_ (должность)

\_\_\_\_\_ (фамилия, имя, отчество)

действующего на основании

в связи с

\_\_\_\_\_ (причина отзыва сертификата)

просит аннулировать (отозвать) сертификат ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО», содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
CommonName (CN)	Общее имя – Фамилия, Имя, Отчество
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
Locality (L)	Город
State (S)	Область
Country (C)	Страна

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Подпись владельца сертификата ключа подписи

\_\_\_\_\_ / \_\_\_\_\_ /

Подпись руководителя организации

\_\_\_\_\_ / \_\_\_\_\_ /

М.П. (при наличии)