

Условия поставки Смарт-ключей Клиентам ООО «БМВ Банк»

г. Новосибирск, 2026 г.

Закрытое акционерное общество «Центр
Цифровых Сертификатов» (именуемое в
дальнейшем «Удостоверяющий центр»)

Директор Гудков А. В.



01 июня 2026 г.

1. Настоящие Условия поставки Смарт-ключей Клиентам ООО «БМВ Банк» (далее – «Условия») являются типовыми для Клиентов ООО «БМВ Банк» (далее по тексту – «Клиенты») и определяют положения договора присоединения для ограниченного круга лиц, заключаемого между Удостоверяющим центром и Клиентом, устанавливающего порядок предоставления Клиентам Смарт-ключа в качестве технологии хранения ключей электронной подписи. В случае, если отдельные термины и определения не установлены настоящими Условиями, применяются термины и определения, определенные Правилами работы Удостоверяющего центра «AUTHORITY».
2. Настоящие Условия размещаются Удостоверяющим центром в сети Интернет на сайте Удостоверяющего центра по адресу: www.authority.ru.
3. Под Клиентами для целей настоящих Условий понимаются юридические лица, зарегистрированные на территории Российской Федерации, и заключившие с ООО «БМВ Банк» договор банковского счета и/или иной договор, предусматривающий электронный документооборот между ООО «БМВ Банк» и юридическим лицом.
4. Предоставление Клиентам Смарт-ключей осуществляется Удостоверяющим центром на основе Заявки по форме Приложения № 1 к Условиям.
5. Наименование Смарт-ключей, допустимых к поставке на основании настоящих Условий, размер вознаграждения Удостоверяющего центра за поставку Смарт-ключей, оказание услуг по предперсонализации Смарт-ключей, включающего расходы на их доставку Клиенту, указаны в Тарифах (Приложение № 2 к Условиям).
6. Настоящие Условия в совокупности с Заявкой и Тарифами содержат все существенные условия, необходимые для заключения договора присоединения.
7. Заключение договора присоединения осуществляется путем присоединения Клиента к договору в соответствии со ст. 428 Гражданского Кодекса Российской Федерации, и производится путем предоставления Клиентом надлежащим образом оформленной и подписанной Заявки в офис ООО «БМВ Банк». Подписание и предоставление Клиентом Заявки означает принятие им настоящих Условий, включая Тарифы и обязательство неукоснительно их соблюдать. Договор считается заключенным с даты получения ООО «БМВ Банк» Заявки Клиента, если иной порядок заключения Договора не установлен законодательством Российской Федерации.
8. Отдельные услуги могут предоставляться Удостоверяющим центром на основании отдельно заключенных с Клиентом соглашений, не предусмотренных настоящими Условиями. Положения таких соглашений имеют преимущество перед положениями настоящих Условий.
9. На основании Заявки Клиента Удостоверяющий центр производит предперсонализацию Смарт-ключей. Количество предперсонализированных Смарт-ключей, подлежащих поставке Удостоверяющим центром Клиенту, определяется в Заявке, направляемой Клиентом Удостоверяющему центру посредством предоставления в офис ООО «БМВ Банк». Предперсонализация Смарт-ключей осуществляется Удостоверяющим центром при наличии технической возможности.
10. После предоставления Заявки Клиент в безналичной форме перечисляет Удостоверяющему центру полную стоимость заказанных им Смарт-ключей по банковским реквизитам Удостоверяющего центра, указанным в Приложении № 3 к настоящим Условиям, указав в назначении платежа «Оплата от *Название организации* за *Наименование Смарт-ключа* согласно Условиям поставки Смарт-ключей Клиентам ООО «БМВ Банк», в том числе НДС _____ руб.».

11. Срок отправки Смарт-ключей Клиенту по Заявке составляет не более 2 (Двух) месяцев, следующих за днём оплаты по соответствующей Заявке.
12. Днём оплаты признается день зачисления подлежащей суммы денежных средств на расчетный счет Удостоверяющего центра, указанный в Приложении № 3 к Условиям.
13. Обязательство Удостоверяющего центра по отправке и передаче Смарт-ключей Клиенту считается выполненным с момента передачи Удостоверяющим центром Смарт-ключей транспортной организации (в т.ч. организации, оказывающей транспортно-экспедиторские услуги). С этого же момента к Клиенту переходит право собственности на Смарт-ключи и риск случайной гибели Смарт-ключей.
14. Клиент обязан подтвердить Удостоверяющему центру факт получения Смарт-ключей в сроки и способом, указанным в сопроводительном письме, которое прилагается Удостоверяющим центром к Смарт-ключам при их отправке. Если в указанный в сопроводительном письме срок Клиент не подтвердит получение Смарт-ключей, Удостоверяющий центр направит Клиенту запрос о подтверждении факта получения Смарт-ключей в электронной форме с адреса электронной почты token@authority.ru по адресу электронной почты ответственного лица Клиента, указанному в Заявке. В таком случае Клиент обязан подтвердить получение Смарт-ключей в сроки и способом, указанным в таком запросе.
15. Гарантийный срок на Смарт-ключи Рутокен составляет 1 (Один) год с даты поставки Смарт-ключей Клиенту.
16. Претензии, связанные с качеством Смарт-ключей, Клиент вправе предъявлять Удостоверяющему центру. Для этого Клиент отправляет Смарт-ключи почтой заказным отправлением с уведомлением о вручении в адрес Удостоверяющего центра, указанный в Приложении №3 к настоящим Условиям, приложив к нему заявление с описанием претензии к качеству Смарт-ключей и запросом на проведение экспертизы по форме Приложения №4 к настоящим Условиям.
17. Документом, подтверждающим факт и дату приема Удостоверяющим центром от Клиента Смарт-ключа на экспертизу, является уведомление о вручении заказного письма, предоставляемое Клиенту службой почтовой доставки по факту вручения отправленного Смарт-ключа Удостоверяющему центру.
18. Удостоверяющий центр обязуется направить Смарт-ключи Производителю для проведения экспертизы. Производитель проводит экспертизу Смарт-ключа в срок не позднее 2 (Двух) месяцев с даты получения Смарт-ключа на экспертизу. По итогам экспертизы Удостоверяющий центр направляет Клиенту заключение о результатах экспертизы, а также в случае подтверждения неработоспособности Смарт-ключа прилагает к почтовому отправлению новый Смарт-ключ взамен отправленного Клиентом, в случае неподтверждения прилагает к почтовому отправлению направленный Клиентом на экспертизу Смарт-ключ.
19. Спецификация на Смарт-ключ, подлежащий к поставке на дату публикации настоящей редакции Условий, приведена в Приложении № 5 к настоящим Условиям. Удостоверяющий центр вправе в одностороннем порядке изменять спецификацию. Информацию о новой спецификации Удостоверяющий центр размещает в сети Интернет по адресу: www.authority.ru. С даты размещения по вышеуказанному адресу новой спецификации, поставка Смарт-ключей, указанных в Тарифах, осуществляется исключительно в соответствии с новой спецификацией.
20. Удостоверяющий центр имеет право в одностороннем порядке изменять положения настоящих Условий. Новая редакция Условий размещается Удостоверяющим центром на сайте Удостоверяющего центра по адресу www.authority.ru не позднее, чем за 5 (Пять) календарных дней до вступления в силу новой редакции Условий. Новая редакция Условий вступает в силу по истечении 5 (Пяти) календарных дней со дня ее публикации на сайте Удостоверяющего центра по адресу www.authority.ru.
21. В случае, если Клиентом в Заявке на поставку Смарт-ключей указаны какие-либо персональные данные, то оператором таких персональных данных является Клиент. В таком случае Клиент гарантирует Удостоверяющему центру, что он получил все необходимые согласия на обработку и передачу Удостоверяющему центру персональных данных от их субъектов.
22. Любая предварительная оплата по настоящим Условиям не является коммерческим кредитом по смыслу ст. 823 Гражданского кодекса Российской Федерации. Стороны договорились о

неприменении к правоотношениям Сторон положений ст. 317.1 Гражданского кодекса Российской Федерации в части начисления законных процентов.

23. Приложения к Условиям:

- 23.1. Приложение № 1: Форма Заявки на поставку Смарт-ключей и их предперсонализацию;
- 23.2. Приложение № 2: Тарифы;
- 23.3. Приложение № 3: Реквизиты ЗАО «ЦЦС»;
- 23.4. Приложение № 4: Заявка на проведение экспертизы Смарт-ключа;
- 23.5. Приложение № 5: Спецификация СКЗИ «Рутокен ЭЦП 3.0 3120»

Тарифы

1. Вознаграждение Удостоверяющего центра за поставку одного Смарт-ключа и оказание услуг по предперсонализации одного Смарт-ключа, включающее расходы на доставку Смарт-ключа до Клиента, составляет:

Наименование Смарт-ключа	Цена, кроме того НДС, руб.*
СКЗИ «Рутокен ЭЦП 3.0 3120»	3 800,00

* НДС по ставке, установленной действующим законодательством Российской Федерации

Реквизиты ЗАО «ЦЦС»

Закрытое акционерное общество «Центр Цифровых Сертификатов» (ЗАО «ЦЦС»)

Адрес в ЕГРЮЛ:

630055, Новосибирская область, г. Новосибирск, ул. ул. Мусы Джалиля, 11, каб.309

Почтовый адрес:

630055, Новосибирская область, г. Новосибирск, ул. ул. Мусы Джалиля, 11

Банковские реквизиты:

Р/с 40702810300000000075 в РНКО «Платежный Центр» (ООО)

БИК 045004832

К/с 30103810100000000832 в Сибирском ГУ Банка России

ИНН 5407187087

КПП 540801001

тел/факс: 8 (383) 336-49-49; 8 (383) 339-92-30

**Приложение №4
к Условиям поставки Смарт-ключей
Клиентам ООО «БМВ Банк»**

Форма заявления от Клиента на экспертизу

Директору ЗАО «ЦС»

Гудкову А.В.

От _____

Заявка на проведение экспертизы Смарт-ключей

Прошу осуществить экспертизу прилагаемых *Наименование Смарт-ключа* в количестве *Количество числом* (Количество прописью).

(наименование организации/индивидуального предпринимателя, либо ФИО Клиента-физического лица).

(указать причину, по которой СКЗИ «Рутокен ЭЦП 3.0 3120» передается на экспертизу).

Контактные данные представителя Клиента (не заполняется для физического лица):	
Информация о Клиента:	_____ (наименование организации/индивидуального предпринимателя, либо ФИО Клиента – физического лица)
	_____ (Ф.И.О. ответственного лица, контактный телефон, e-mail)
	_____ (почтовый адрес)

Подписано от Клиента
_____ (_____)
М.П.

Рутокен ЭЦП 3.0 3120, серт. ФСБ

- USB-устройство с аппаратной реализацией: ГОСТ Р 34.10-2012 с длиной ключа 256/512 бит и ГОСТ Р 34.11-2012, а также новых симметричные шифров Магма и Кузнечик и международных алгоритмов электронной подписи RSA и ECDSA. Криптографические операции выполняются без копирования ключа в память компьютера.
- Интерфейс: USB 1.1 и выше.
- Объем EEPROM память (не менее): 128 Кбайт
- Аппаратная реализация алгоритмов ГОСТ Р 34.10-2012/ГОСТ 34.10-2018 (256 и 512 бит): генерация ключевых пар с проверкой качества, формирование и проверка электронной подписи, срок действия закрытых ключей до 3-х лет.
- Аппаратная реализация алгоритмов ГОСТ Р 34.11-2012/ГОСТ 34.11-2018 (256 и 512 бит): вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования ЭП.
- ГОСТ Р 34.12-2015/ГОСТ 34.12-2018 (**Кузнечик**): генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ).
- ГОСТ Р 34.12-2015/ГОСТ 34.12-2018 (**Магма**): генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ).
- Выработка сессионных (ключей парной связи):
 - по схеме VKO GOST R 34.10-2012 (RFC 7836);
 - расшифрование по схеме EC El-Gamal.
- RSA: поддержка ключей размером 1024, 2048, 4096 бит, генерация ключевых пар с настраиваемой проверкой качества, импорт ключевых пар, формирование электронной подписи.
- ECDSA с кривыми secp256k1, secp256r1 и secp384r1, secp521r1: генерация ключевых пар с настраиваемой проверкой качества, импорт ключевых пар, формирование электронной подписи.
- Генерация последовательности случайных чисел требуемой длины.
- Двухфакторная аутентификация: по предъявлению самого идентификатора и по предъявлению уникального PIN-кода.
- Поддержка 3 категорий владельцев: Администратор, Пользователь, Гость.
- Поддержка 2-х Глобальных PIN-кодов: Администратора и Пользователя.
- Поддержка Локальных PIN-кодов для защиты конкретных объектов (например, контейнеров сертификатов) в памяти устройства.

- Настраиваемые аппаратные политики качества PIN-кодов, обрабатываются микропрограммой при соответствующих операциях. Устанавливаются при форматировании, опционально могут изменяться позднее по PIN-коду Администратора;
- Варианты политик:
 - Ограничение минимальной длины PIN-кода;
 - Ограничение использования PIN-кода по умолчанию;
 - Запрет PIN-кода, состоящего из одного повторяющегося символа;
 - Независимые требования по наличию в PIN-коде: прописных, строчных букв латинского и русского алфавитов; цифр; специальных символов;
 - Запоминание до 10 устанавливаемых значений PIN-кода, и возможность запрета установки ранее использованного PIN-кода.
- Поддержка комбинированной аутентификации: по схеме «Администратор или Пользователь» и аутентификация по Глобальным PIN-кодам в сочетании с аутентификацией по Локальным PIN-кодам.
- Создание локальных PIN-кодов для дополнительной защиты части ключевой информации, хранящейся на USB-токене. Возможность одновременной работы с несколькими локальными PIN-кодами (до 7 шт.).
- Ограничение числа попыток ввода PIN-кода.
- Индикация факта смены Глобальных PIN-кодов по умолчанию на оригинальные.
- Протокол обмена по ISO/IEC 7816-12.
- Интерфейс подключения USB CCID: работа без установки драйверов устройства в современных версиях ОС.
- Поддержка PC/SC.
- Microsoft Crypto API.
- Microsoft SmartCard API.
- PKCS#11 (включая российский профиль).
- Современный защищенный микроконтроллер.
- Идентификация с помощью 32-битного уникального серийного номера.
- Поддержка операционных систем: Microsoft Windows 2022/11/10/8.1/2019/2016/2012R2/8/2012/7/2008R2; GNU/Linux (в том числе отечественные); Apple macOS 10.13 и новее; iOS/iPadOS 16.2 и новее; Android 7 и новее; Аврора 4+
- Работа с СКЗИ «КриптоПро CSP 5.0 R2» и новее по протоколу защиты канала SESPake (ФКН2).
- Собственный CSP со стандартным набором интерфейсов и функций API.
- Minidriver для интеграции с Microsoft Base Smart Card Cryptographic Service Provider.
- Журналирование операций электронной подписи, сформированных по ГОСТ-алгоритмам, фиксация параметров электронной подписи и окружения.
- Ведение неубывающего счетчика операций электронной подписи в рамках журнала.

- Доверенное получение журнала, подтвержденное электронной подписью.
- Журнал событий безопасности, в котором фиксируются: Операции форматирования; Удаление/генерация любых неизвлекаемых ключей, созданных через библиотеки Рутокен (PKCS#11, Aktiv ruToken CSP, minidriver), а также ФКН-контейнеры КриптоПро CSP 5.0+; Смена PIN-кодов Пользователя/Администратора.
- Контроль целостности микропрограммы (прошивки) Рутокен ЭЦП.
- Контроль целостности системных областей памяти.
- Проверка целостности RSF-файлов перед любым их использованием.
- Счетчики изменений в файловой структуре и изменений любых PIN-кодов для контроля несанкционированных изменений.
- Проверка правильности функционирования криптографических алгоритмов.
- Наличие действующего сертификата соответствия выданного ФСБ РФ, удостоверяющего, что СКЗИ соответствует требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащих сведений, составляющих государственную тайну, классов КС1, КС2 и удовлетворяет требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2001г. №796, установленным для класса КС1, КС2 и может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.
- Реализация криптографического функционала должна быть максимально безопасной: необходимые алгоритмы должны изначально присутствовать в микропрограмме, а не добавляться дополнительными загружаемыми модулями (апплетами, плагинами и т.п.).

Наличие сертификата соответствия ФСБ.