Приложение
к Приказу Генерального директора ООО «Атомайз»
от 17.08.2021 г. № АТМ/17.08.2021/1-п

Требования к валидаторам

1. Общие положения.

1.1. Настоящие Требования разработаны в целях принятия Оператором информационной системы решения о допуске Валидатора к подтверждению Транзакций или об отказе в таком допуске на Платформе ООО «Атомайз».

1.2. Настоящие Требования определяют требования к Валидаторам в зависимости от типа узлов валидации, требования к наличию у Валидаторов программного обеспечения и оборудования, необходимого для подтверждения Транзакций, а также требования к обеспечению защиты информации на узлах валидации.

1.3. Основные положения настоящих Требований раскрываются на сайте https://atomyze.ru.

1.4. Требования, содержащиеся в настоящем документе, могут быть изменены по соглашению сторон в рамках договора на оказание услуг валидации.

2. Термины и определения

Термин	Определение
Валидатор	Юридическое лицо, зарегистрированное в соответствии с законодательством Российской Федерации.
Оператор информационной системы (Оператор)	Общество с ограниченной ответственностью «Атомайз» (ОГРН 1207700427714), действующее в качестве оператора информационной системы в соответствии Федеральным законом от 31.07.2020 N 259-ФЗ "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации" и включенное Банком России в реестр операторов информационных систем.
Ордерер	Узел валидации, который в рамках подтверждения Транзакций осуществляет функционал по формированию блоков Транзакций для их последующей записи Пирами в Информационную систему.
Пир	Узел валидации, который в рамках подтверждения операций с ЦФА осуществляет функционал по записи сформированных Ордерером блоков Транзакций в Информационную систему.
Платформа	Программное обеспечение, которое включает Информационную систему и иные сопутствующие программные модули, обеспечивающие возможность

	взаимодействия Пользователя с Информационной системой. Платформа доступна на Сайте Оператора информационной системы или посредством Мобильного приложения.
Транзакция	Операция по переходу ЦФА, осуществляемая в Информационной системе.
ФЗ о ЦФА	Федеральный закон № 259-ФЗ от 31.07.2020 "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации".
ЦФА	Цифровой финансовый актив (по смыслу ч. 2 ст. 1 ФЗ о ЦФА) и(или) цифровое право, включающее одновременно цифровые финансовые активы и иные цифровые права (по смыслу части 6 ст. 1 ФЗ о ЦФА), которые выпускаются и учитываются в Информационной системе в соответствии с ФЗ о ЦФА, иными требованиями законодательства, Правилами информационной системы, которым соответствует определенный Смарт-контракт.
Эндорсер	Узел валидации, который в рамках подтверждения Транзакций осуществляет функционал по проверке приватных ключей и балансов кошельков Пользователей, передаче Транзакций Ордерерам для формирования блоков Транзакций.

Иные термины и определения имеют значение, указанное в Правилах оператора информационной системы, размещенных на сайте Оператора информационной системы.

3. Требования к Валидаторам:

3.1. Валидатором Платформы может быть юридическое лицо, а также зарегистрированный в соответствии с законодательством Российской Федерации индивидуальный предприниматель.

3.2. Валидатор должен владеть ЦФА определенного выпуска и (или) вида.

4. Требования к программному обеспечению и оборудованию, необходимому для подтверждения Транзакций

4.1. Оборудование:

№	Тип узла валидации	Количество виртуальных ядер vCPU	Объем оперативной памяти, Gb	Объем жесткого диска, Gb	Тип жесткого диска
1.	Пир	4	16	1024	HDD
2.	Ордерер	4	16	1024	HDD
3.	Эндорсер	4	16	1024	HDD

4.2. Для поддержания работоспособности и отказоустойчивости аппартные и программные средства валидации должны дублироваться и в случае сбоя основного комплекса переключаться на резервные узлы.
4.3. ЦОД Валидатора должен соответвовать Уровню II и выше по классификации отказоустойчивости:

- Уровень I — базовая инфраструктура без резервирования;
- Уровень II — инфраструктура с резервными мощностями;
- Уровень III — инфраструктура, поддерживающая параллельный ремонт;
- Уровень IV — отказоустойчивая инфраструктура.

4.4. Аппаратные и программыне средства Валиатора должны быть защищены средствами противодействия DDoS-атакам.
4.5. Валидатору необходимо предусмотреть дублирование каналов связи, используемых для подключения аппаратно-программных средств к сети валидации.
4.6. Валидатору необходимо производить тестирование работоспособности всех компонентов аппаратно-программых средств перед подключением к сети Оператора информационной системы.
4.7. Аппаратно-программные средства валидации должны быть подключены к системе непрерывного мониторинга работы узлов для своевременного выявления сбоев и уведомления персонала Валидатора и персонала Оператора информационной системы о неработоспособности узла Валидатора с целью скорейшего восстановления работы.
4.8. Инциденты и аварии, произошедшие в аппаратно-программной среде Валидтора, должны регистрироваться с системе учета событий операционной надежности Оператора информационной системы и по итогам устранения должны формироваться отчеты о причинах возникновения сбоев и аварий, методах их устранения и мероприятий по недопущению возникновения данных ситуаций в будущем.

5. Требования к обеспечению защиты информации

5.1. Валидатору необходимо использовать на серверах валидации только лицензированное программное обеспечение и своевременно производить обновления ПО операционной системы и прикладного ПО для закрытия уязвимостей информационной безопасности.
5.2. Валидатору необходимо использовать сетевой экран для защиты от несанкционированного доступа к аппаратным и программным средствам валидации.
5.3. Валидатору запрещается проводить анализ программного обеспечения поставляемого Оператором информационной системы и осуществлять реверс-инжениринг кода программного обеспечения.
5.4. Валидатору необходимо в обязательном порядке соответствовать актуальным требованиям законодательства к сети Оператора информационной системы в части операционной надежности и информационной безопасности.

6. Тербования к операционной надежности

Валидатор обязан соблюдать следующие требования:

6.1. Поддерживать работоспособность узла валидации и его подключения к сети Оператора информационной системы на уровне доступности 95% общего времени работы;
6.2. Реагировать на сбой в работе узла валидации приведшего к недоступности узла или некорректной работы в течение 15 минут с момента получения оповещения о неработоспособности узла от систем мониторинга или от любого участника сети валидации Оператора информационной системы;
6.3. Восстанавливать работоспособность узла валидации не менее чем за 2 часа с момента обнаружения факта недоступности или некорректной работы узла;
6.4. В течении 3 (трех) рабочих дней с момента возникновения инцидента связанного с неработоспособностью или некорректной работой узла валидации предоставлять Оператору информационной системы отчет о причинах возникновения инцидента и мерах по восстановлению и предотвращению подобных инцидентов.