



Ассоциация банков России
(Ассоциация «Россия»)

ПРЕЗИДЕНТ

125009, Москва, Никитский пер., д.4, стр. 1

www.asros.ru

asros@asros.ru

т. 8-(495)-785-29-90

**Генеральному директору
ППК «Роскадастр»**

Т.А. Громовой

от 05.06.2026 № 02-05/646

*О вопросах эксплуатации банками
СВР и АЭВ*

Уважаемая Татьяна Алексеевна!

Ассоциация банков России в связи с обращениями кредитных организаций направляет в ППК «Роскадаст» информацию о проблемах и вопросах, возникших при внедрении и в ходе эксплуатации программного обеспечения Сервиса взаимодействия с Росреестром и Адаптера электронного взаимодействия¹ в банках.

1. Использование физических носителей электронной подписи клиентов.

Согласно описанию функциональности АЭВ, подписание документов предполагает использование электронной подписи пользователя, размещенной на физическом носителе.

На практике сценарий взаимодействия с клиентом предполагает, что сотрудник банка в ПО СВР и АЭВ формирует заявления («пакеты», «сделки»), прикладывает необходимые документы, после чего клиент использует свой съемный носитель (РуТокен с УКЭП) для подписания документов на автоматизированном рабочем месте сотрудника банка.

При этом использование внешних съемных носителей в информационных системах кредитных организаций строго регламентируется требованиями информационной безопасности и находится под контролем Банка России, в том числе в рамках ГОСТ Р 57580.1-2017, а также внутренними процедурами банков по обеспечению информационной безопасности².

В этой связи просим сообщить, предусматриваются ли ППК «Роскадаст» и Росреестром альтернативные сценарии подписания документов, исключающие необходимость использования клиентских физических носителей электронной подписи на рабочих местах сотрудников банков.

¹ Далее – СВР и АЭВ.

² Фактическое использование клиентских носителей электронной подписи на автоматизированных рабочих местах сотрудников банка в большинстве случаев невозможно без проведения предварительных процедур регистрации, проверки и допуска таких носителей средствами информационной безопасности банка.

2. Организация пользовательского доступа.

Создание отдельных учетных записей под каждого клиента в информационных системах кредитных организаций создает значительную административную и операционную нагрузку, связанную с процедурами предоставления, изменения и прекращения доступа клиентам, с учетом необходимости соблюдения внутренних требований банков к информационной безопасности.

В этой связи просим сообщить, существуют ли рекомендуемые сценарии организации пользовательского доступа, позволяющие минимизировать необходимость создания отдельных учетных записей для клиентов.

3. Использование УКЭП ГосКлюч представителем юридического лица.

У кредитных организаций отсутствует понимание, допускается ли использование сценария, при котором документы подписываются посредством УКЭП ГосКлюч уполномоченным физическим лицом, действующим от имени юридического лица, с приложением доверенности либо иных документов, подтверждающих полномочия представителя.

Просим разъяснить, соответствует ли указанный сценарий требованиям Росреестра и архитектуре СВР и АЭВ.

4. Техническая поддержка и сопровождение СВР и АЭВ.

По информации банков, обновления программного обеспечения предоставляются ППК «Роскадастр» без подробного описания состава изменений, что увеличивает трудоемкость анализа доработок, тестирования и внедрения обновлений в продуктивную среду.

Кроме того, отмеченные банками длительные сроки рассмотрения обращений и устранения технических инцидентов³ затрудняют оперативное обслуживание клиентов и настройку взаимодействия с сервисом.

В этой связи просим учесть данные замечания при совершенствовании сопровождения СВР и АЭВ.

Будем признательны за позицию ППК «Роскадастр» по указанным вопросам, а также содействие в повышении функциональности сервиса и развитие механизмов оперативного взаимодействия кредитных организаций по вопросам его эксплуатации.

С уважением,

Д.Г. Липаев

³ Средняя скорость ответа составляет 6-7 дней, решение проблемы может занимать до 1 месяца.