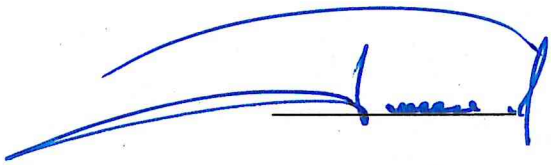
Дата: «13» 03 2026г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
ПРОВЕДЕНИЕ СЕРТИФИКАЦИОННОГО АУДИТА

Наименование:
«Проведение сертификационного аудита для соответствия требованиям международного стандарта PCI 3DS Security Requirements для АО «Milliy Banklararo Protsessing Markazi»»

Заказчик: АО «Национальный Межбанковский Процессинговый Центр» (НМПЦ)
Контактное лицо: Тоиров А. (Главный специалист отдела по закупкам, +998781132407 / 7733, tender@nmpc.uz)

Согласовано:
Председатель правления
Бахадиров У. Х.



Директор департамента ИБ
Гафуров А. А.

Разработал:
Ведущий специалист отдела анализа уровня обеспечения информационной безопасности, расследований и оценки ущерба от событий и инцидентов информационной безопасности
Зубайдуллаев Ж. Ш.

Техническое задание

для проекта

Проведение сертификационного аудита для соответствия требованиям международного стандарта PCI 3DS Security Requirements для АО «Milliy Banklararo Protsessing Markazi»

Ташкент 2026 г.

1. ТРЕБОВАНИЯ К УСЛУГАМ

1.1. Полное наименование предмета работ

Проведение сертификационного аудита для соответствия требованиям международного стандарта PCI 3DS Security Requirements для АО «Milliy Banklararo Protsessing Markazi».

1.2. Границы оказания услуг

В границы оказания услуг должны входить площадки Заказчика, содержащие среду данных платежных карт и сервисы 3DS инфраструктуры в г. Ташкент, Узбекистан, включая следующие типы оказываемых услуг:

- POS-processing;
- ATM - processing.

Расширение границ оказания Услуг закрепляется дополнительным соглашением сторон.

1.3. Перечень документов, на основании которых оказываются услуги

Все предлагаемые услуги должны оказываться в полном соответствии со следующей нормативной документацией:

- PCI 3DS Security Requirements 1.0;

а также дополнительными инструкциями, получаемыми от платежных систем.

2. Требования к Исполнителю

Исполнитель должен иметь действующий статус в регионе CEMEA - 3DS Assessor (3DS), позволяющий проводить работы в регионе. Актуальность статуса 3DS Исполнителя в регионе CEMEA должен быть подтверждена письмом участника с приведением скрина нахождения участника в актуальном списке сертифицированных аудиторов Payment Card Industry Security Standards Council (PCI SSC).

Исполнитель должен предоставить подтверждение опыта о не менее 3-х завершенных проектах по оценке соответствия требованиям стандартов PCI DSS или PCI 3DS за последние 3 (три) года (результаты приняты МПС и выданы сертификаты соответствия) в финансовом секторе стран СНГ. Подтверждается копиями Актов оказания услуг или УПД, счет-фактуры, отзывами, благодарностями от Заказчиков (допускается сокрытие конфиденциальной информации, но из представленных документов должны определяться: дата договора, предмет оказания услуг, наименование заказчика, подписи сторон).

Опыт завершенных проектов по оценке соответствия требованиям стандарта PCI DSS или PCI 3DS (результаты приняты МПС и выданы сертификаты соответствия), проведенных на территории Республики Узбекистан, будет преимуществом.

Исполнитель должен предоставить подтверждение наличия в команде сертифицированных специалистов, обладающих статусом Qualified Security Assessor (QSA) – не менее 3 (Копия сертификатов специалистов);

Исполнитель должен предоставить подтверждение наличия в команде сертифицированных специалистов, обладающих статусом 3DS Assessors (3DS) – не менее 1 (Копия сертификата специалиста);

Исполнитель должен предоставить подтверждение наличия в команде сертифицированных специалистов, обладающих статусом Secure Software Assessor (SSA) – не менее 1 (Копия сертификата специалиста);

Исполнитель должен предоставить подтверждение наличия в команде сертифицированных специалистов, обладающих статусом Secure SLC Assessor (SSLCA) – не менее 1 (Копия сертификата специалиста);

Исполнитель должен предоставить подтверждение наличия в команде сертифицированных специалистов, обладающих статусом Certified Information Systems

Security Professional (CISSP) или Certified Information Systems Auditor (CISA) – не менее 2 (Копия сертификатов специалистов);

Исполнитель должен предоставить подтверждение наличия в команде специалистов, обладающих статусом BSI ISO/IEC 27001 Lead Auditor – не менее 2 (Копия сертификатов специалистов);

Исполнитель должен предоставить подтверждение наличия в команде специалистов, обладающих статусом BSI ISO/IEC 27001 Lead Implementer – не менее 1 (Копия сертификатов специалистов).

3. Состав и описание оказываемых услуг

3.1. Предварительный сбор и анализ исходных данных

На данном этапе должен осуществляться сбор и анализ предварительной информации о составе используемых ключей шифрования, используемом оборудовании, контактную информацию офицеров безопасности и другую необходимую информацию.

Для этого Исполнитель должен передать Заказчику анкету предварительного запроса информации, а Заказчик заполняет ее по мере возможности, после чего возвращает Исполнителю по электронной почте для ознакомления.

3.2. Проведение аудита и формирование «PCI 3DS Report on Compliance»

На данном этапе оказываемых услуг аудиторы Исполнителя на площадке Заказчика должны проводить необходимое интервьюирование ответственных сотрудников Заказчика, проверять параметры безопасности системных компонент, участвующих в процессах обработки данных 3-D Secure операций, и документировать свидетельства аудита.

Сбор всех необходимых сведений должно производиться путем изучения нормативной документации, предоставляемой Заказчиком, проведения интервью, анализа конфигурационных файлов, демонстрирования сотрудниками Заказчика выполняемых ими процедур по обеспечению информационной безопасности.

Разработка «PCI 3DS Report on Compliance» должна осуществляться Исполнителем на основе собранных свидетельств аудита и в соответствии с требованиями PCI 3DS Security Requirements, такими как:

1. Управление безопасностью.
2. Защита 3DS систем и приложений.
3. Безопасный логический доступ к системам 3DS.
4. Защита данных 3DS.
5. Криптография и управление ключами.
6. Физическая безопасность систем 3DS.

Результатом оказания услуг на данном этапе должно являться PCI 3DS Report on Compliance (PCI 3DS ROC).

3.3. Сопровождение при устранении выявленных несоответствий

В случае выявления несоответствий, Заказчик должен принять необходимые для их устранения меры и задекларировать (подтвердить) данный факт аудиторам Исполнителя. Для этого, в зависимости от типа и характера несоответствия, возможно:

- Предоставление подтверждающих документов (регламент, политика, журнал, скриншот и т.п.) по электронной почте;
- Демонстрация процедур на месте;
- Другие подтверждающие мероприятия.

3.4. Формирование PCI 3DS Attestation of Compliance

В случае получения свидетельств, подтверждающих факт устранения всех выявленных несоответствий в срок до 90 календарный дней с даны получения PCI 3DS ROC – Исполнитель должен формировать PCI 3DS Attestation of Compliance (PCI 3DS AOC).

Подписанный Сторонами PCI 3DS AOC должен направляться Исполнителем в международные платежные системы для подтверждения успешного завершения аудита по требованиям PCI 3DS Security Requirements 1.0.

3.5. Оказание консультационной поддержки по вопросам выполнения требований стандарта

Целью оказания услуг на данном этапе должно являться консультирование специалистов Заказчика по возникающим вопросам, связанным с разъяснением конкретных требований Стандарта и способам их выполнения.

Консультационная поддержка Заказчика должна осуществляться Исполнителем в течение 1 года с момента заключения договора. Прием запросов должно осуществляться по электронной почте и телефону. Время ответа на каждый поступивший запрос может составлять от 1 до 5 рабочих дней, в зависимости от сложности запроса.