



**ФАРМОИШИ
ДИРЕКТОРИ АГЕНТИИ ИННОВАТСИЯ ВА ТЕХНОЛОГИЯҲОИ
РАҚАМИИ НАЗДИ ПРЕЗИДЕНТИ ҶУМҲУРИИ ТОҶИКИСТОН**

Аз «10» феврал соли 2025

№ 1/01

ш. Душанбе

**О Порядке приобретения и использования корневых сертификатов
защищенных электронных подписей**

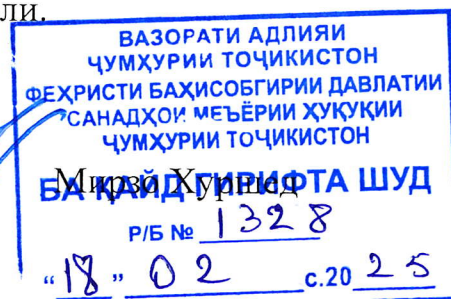
180.080.040.

В соответствии со статьёй 6 Закона Республики Таджикистан «Об электронном документе и электронной подписи» и пунктом 10 Положения об Агентстве инноваций и цифровых технологий при Президенте Республики Таджикистан, утвержденного указом Президента Республики Таджикистан от 27 марта 2024 года, №798,

РАСПОРЯЖАЮСЬ:

1. Утвердить Порядок приобретения и использования корневых сертификатов защищенных электронных подписей (прилагается).
2. Настоящее распоряжение представить в Министерство юстиции Республики Таджикистан для государственной регистрации и ввести в действие после государственной регистрации и официального опубликования.
3. Финансово-хозяйственному отделу после государственной регистрации принять меры для официального опубликования настоящего распоряжения в газете «Джумхурият».
4. Управлению регулирования оборота электронного документа и электронной подписи совместно с Открытым акционерным обществом «Удостоверяющие центры, государственные услуги и разработка цифровых программ» в соответствии с настоящим Порядком осуществлять приобретения и использование корневых сертификатов защищенных электронных подписей.
5. Контроль за исполнением настоящего распоряжения возложить на заместителя директора Агентства инноваций и цифровых технологий при Президенте Республики Таджикистан – куратора отрасли.

Директор Агентства инноваций
и цифровых технологий при
Президенте Республики Таджикистан



Порядок приобретения и использования корневых сертификатов
защищенных электронных подписей

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Порядок приобретения и использования корневых сертификатов защищенных электронных подписей (далее – настоящий Порядок) устанавливает порядок приобретения и использования корневых сертификатов защищенных электронных подписей.

2. В настоящем Порядке используются следующие основные понятия:

- корневой удостоверяющий центр – уполномоченный орган по государственному надзору в сфере электронной подписи (удостоверяющие центры отправляют информацию о выданных сертификатах в корневой удостоверяющий центр. Проверка подлинности и достоверности электронной подписи осуществляется через корневой удостоверяющий центр, и центр обеспечивает полноту и сохранение информации в непредвиденных обстоятельствах);

- удостоверяющий центр - юридическое лицо, имеющее право проверить соответствие открытого ключа защищенной электронной подписи закрытому ключу защищенной электронной подписи;

- корневой сертификат защищенной электронной подписи (далее-корневой сертификат) - файл, в котором помещена информация корневого удостоверяющего центра, в том числе имя, идентификационный номер налогоплательщика, адрес, срок действия и алгоритм шифрования и передаётся в удостоверяющему центру.

2. ПОРЯДОК ПРИОБРЕТЕНИЯ КОРНЕВЫХ СЕРТИФИКАТОВ

3. Приобретение корневых сертификатов осуществляется в целях обеспечения юридической значимости и безопасности электронной подписи оказанию услуги, связанной с использованием защищенной электронной подписи, и проверке подлинности защищенных электронных подписей.

4. Процесс приобретение корневого сертификата осуществляется в соответствии с действующим законодательством.

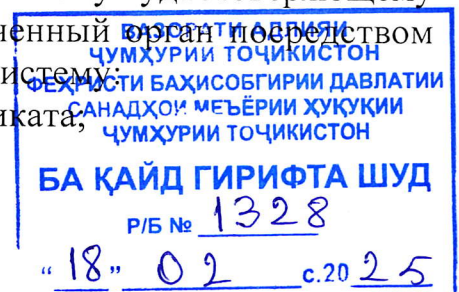
5. Корневые сертификаты приобретаются у корневого удостоверяющего центра, соответствующий международным и государственным стандартам.

6. Приобретения корневых сертификатов состоит из следующих этапов:

1) удостоверяющие центры направляют корневому удостоверяющему следующие документы и информацию в уполномоченный орган посредством почтовой связи, лично или через информационную систему:

- заявление для приобретения корневого сертификата;

-юридическое наименование;



- копия положения (устава);
- цель использования корневого сертификата;
- сведения об информационных системах, где будет применяться корневой сертификат;
- сведения о политике информационной безопасности;
- контактные данные ответственного лица.

2) корневой удостоверяющий центр проверяет документы на соответствие установленным требованиям в срок не более 15 рабочих дней;

3) удостоверяющие центры заключают соглашение с корневым удостоверяющим центром, в котором оговариваются следующие условия:

- права и обязанности сторон;
- срок действия корневого сертификата;
- порядок замены и отзыва корневого сертификата;
- условия обеспечения конфиденциальности;

4) при одобрении заявки удостоверяющий центр уведомляется о возможности получения корневого сертификата.

7. После рассмотрения документов и проверки программного обеспечения и технических возможностей заявителя на соответствие требованиям, предъявляемым к удостоверяющим центрам, корневой удостоверяющий центр выдает удостоверяющему центру корневой сертификат. Информация о получении корневого сертификата фиксируется в корневом удостоверяющем центре.

8. Корневой сертификат передается удостоверяющим центрам через защищенный канал связи, одобренный корневым удостоверяющим центром.

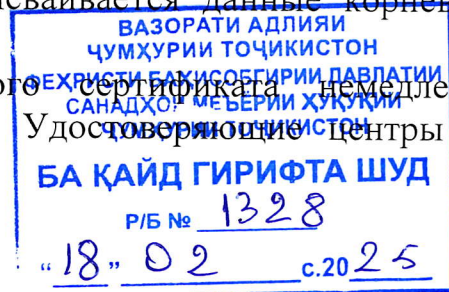
9. При получении корневого сертификата проверяется его правильность путем проверки контрольной суммы и верификация подписи корневого удостоверяющего центра.

10. Корневой сертификат, выдаваемый удостоверяющему центру, должен содержать следующую информацию:

- идентификационные данные, в том числе имя владельца сертификата, название удостоверяющего центра и имя организации;
- имя издателя сертификата (название корневого удостоверяющего центра, организация)
- параметры ключа и шифрования (открытый ключ, алгоритмы подписи);
- информация о корневом сертификате (серийный номер, уникальный номер, присваиваемый сертификату);
- срок действия (дата начала действия корневого сертификата, дата окончания действия корневого сертификата);
- версия сертификата X.509 версии 3.

11. Корневой удостоверяющий центр переподчиняет сертификат удостоверяющего центра, путем предоставления нового сертификата, где в структуре сертификата, в поле издатель, присваиваются данные корневого удостоверяющего центра.

12. В случае компрометации корневого сертификата, немедленно уведомлять корневой удостоверяющий центр. Удостоверяющие центры по



истечении срока действия корневого сертификата для получения следующего корневого сертификата должны обратиться в корневой удостоверяющий центр.

13. Корневой удостоверяющий центр отказывает удостоверяющему центру в выдаче сертификата в следующих случаях:

- неполнота или некорректность представленных документов;
- представления недостоверных сведений и отказ в проверке и сотрудничестве;
- несоответствие требованиям безопасности;
- вступление в законную силу решение суда (решение о ликвидации удостоверяющего центра);
- если программное обеспечение и технические возможности заявителя не соответствуют требованиям корневого удостоверяющего центра.

3. ПОРЯДОК ИСПОЛЬЗОВАНИЯ КОРНЕВЫХ СЕРТИФИКАТОВ

14. Удостоверяющие центры после приобретения должны использовать корневой сертификат исключительно в соответствии с заявленной целью. Корневой сертификат используется для проверки подлинности подписей, установления доверия к сертификатам других участников, также для проверки доверия к электронной подписи, приложенной к документам, и обеспечение криптографической безопасности данных.

15. Корневой удостоверяющий центр и удостоверяющие центры обязаны обеспечить защиту корневого сертификата от несанкционированного доступа, копирования или утраты.

16. Корневой сертификат устанавливается только в доверенные хранилища систем, прошедших проверку на соответствие требованиям информационной и технической безопасности.

17. Любые действия, связанные с использованием корневого сертификата, должны быть задокументированы и доступны для проверки.

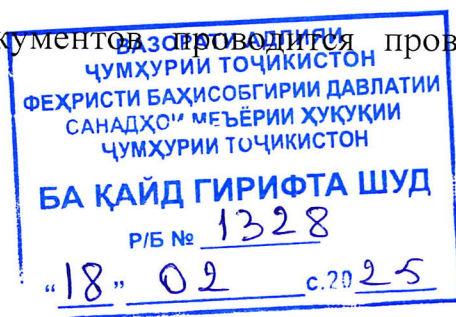
18. Использование корневого сертификата осуществляется строго в соответствии с внутренними актами удостоверяющего центра и законодательными требованиями.

19. Корневой сертификат не используется для подписания документов или выполнения операций, которые не входят в его прямые функциональные обязанности.

20. Корневой сертификат устанавливается на всех устройствах и системах, где требуется проверка подписей. Установка производится уполномоченным сотрудником корневого удостоверяющего центра с использованием следующих шагов:

- импорт сертификата в хранилище доверенных корневых сертификатов (например, в «ОС Windows», «Linux» или специализированных системах);
- проверка корректности установки через стандартные средства проверки корневых сертификатов.

21. При поступлении электронных документов проводится проверка подписи на основе корневого сертификата.



22. Для проверки используется программное обеспечение, поддерживающее установленные алгоритмы и отвечающее требованиям корневого удостоверяющего центра.

23. Доступ к корневому сертификату предоставляется только уполномоченным сотрудникам удостоверяющего центра.

24. В случаях необходимости, для делегирования прав использования корневого сертификата оформляется документ с указанием ответственных лиц и временных ограничений.

4. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

25. За несоблюдение положений настоящего Порядка ответственные лица привлекаются к ответственности в соответствии с законодательством Республики Таджикистан.

