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

Аз «10» февраля соли 2025 № 1/02 ш. Душанбе

О Правилах выдачи, хранения, отзыва сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в частности корневым удостоверяющим центром и удостоверяющими центрами государственных органов

180.080.040.

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

Р А С П О Р Я Ж А Ю С Ь:

1. Утвердить Правила выдачи, хранения, отзыва сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в частности корневым удостоверяющим центром и удостоверяющими центрами государственных органов (прилагаются).

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», удостоверяющие центры и удостоверяющие центры государственных органов в соответствии с настоящими Правилами осуществлять выдачу, хранение, отзыв сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи.

ВАЗОРАТИ АДЛИЯИ ҶУМҲУРИИ ТОҶИКИСТОН
ФЕҲРИСТИ БАҲИСОБГИРИИ ДАВЛАТИИ САНАДҲОИ ҲУҚУҚӢ ҶУМҲУРИИ ТОҶИКИСТОН
БА ҚАЙД ГИРИФТА ШУД
Р/Б № 1329
«28» 02 с.2025

5. Контроль за выполнением 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 Мирзо Хуршед

ВАЗОРАТИ АДЛИЯИ
ҶУМҲУРИИ ТОҶИКИСТОН
ФЕҲРИСТИ БАҲИСОБГИРИИ ДАВЛАТИИ
САНАДҲОИ МЕЪЁРИИ ҲУҚУҚИИ
ҶУМҲУРИИ ТОҶИКИСТОН
БА ҚАЙД ГИРИФТА ШУД
Р/Б № 1325
"28" 02 с.2025

Приложение
к распоряжению директора Агентства
инноваций и цифровых технологий при
Президенте Республики Таджикистан
«___» _____ 2025 года, №___

# Правила выдачи, хранения, отзыва сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в частности корневым удостоверяющим центром и удостоверяющими центрами государственных органов

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Правила выдачи, хранения, отзыва сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в частности корневым удостоверяющим центром и удостоверяющими центрами государственных органов (далее – настоящие Правила) определяют правила выдачи, хранения, отзыва сертификатов и подтверждения принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в частности корневым удостоверяющим центром и удостоверяющими центрами государственных органов.

2. В настоящих Правилах используются следующие основные понятия:

- средство криптографической защиты информации – программное обеспечение или аппаратно-программный комплекс, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение и или управление ключами шифрования;
- заявитель - физические и юридические лица, государственные органы;
- пользователь – физические и юридические лица и работники государственных органов, на имя которых удостоверяющим центром, в частности корневым удостоверяющим центром, удостоверяющими центрами государственных органов выдан сертификат;
- удостоверяющий центр - юридическое лицо, обладающее соответствующими правами на удостоверение соответствия открытого ключа защищенной электронной подписи закрытому ключу защищенной электронной подписи;
- 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 настоящий удостоверяющий центр обеспечивает полноту и сохранение информации в непредвиденных обстоятельствах);
- удостоверяющие центры государственных органов удостоверяющие центры которые обслуживают государственные органы и должностных лиц

государственных органов в информационных системах и иных государственных информационных ресурсах Республики Таджикистан;

- уполномоченный орган - Агентство инноваций и цифровых технологий при Президенте Республики Таджикистан;

-оператор - Открытое акционерное общество «Удостоверяющие центры, государственные услуги и разработка цифровых программ» Агентство инноваций и цифровых технологий при Президенте Республики Таджикистан;

- сертификат - сертификат ключа защищенной электронной подписи;

- реестр - реестр сертификатов ключей защищенной электронной подписи.

3. Государственные удостоверяющие центры оказывают услуги, связанные с защищенными электронными подписями, государственным органам, государственным учреждениям, государственным предприятиям и иным хозяйствующим субъектам.

## 2. ПОРЯДОК ВЫДАЧИ СЕРТИФИКАТА

### §1. Выдача сертификата удостоверяющим центром, в частности корневым удостоверяющим центром

4. Для получения сертификата заявитель представляет следующие документы в удостоверяющий центр, в частности в корневой удостоверяющий центр посредством почтовой связи, лично или через информационную систему:

- заявление для получения сертификата согласно приложению 1 настоящих Правил;

- копию свидетельства о регистрации в налоговом органе, копию учредительных документов и доверенность для юридических лиц;

- копию паспорта (или иной документ, удостоверяющий личность) для физических лиц.

5. Выдача сертификата заявителю осуществляется в течение пяти рабочих дней, после подачи документов, указанных в пункте 4 настоящих Правил. План предоставления оказания услуг по выдаче сертификата осуществляется в соответствии с приложением 3 настоящих Правил.

6. После рассмотрения документов заявителю выдается сертификат, который заносится в реестр.

7. Удостоверяющий центр, в частности корневой удостоверяющий центр отказывает удостоверяющему центру в выдаче сертификата в следующих случаях:

- неполноты представленных документов;

- представления недостоверных сведений;

- вступление в законную силу решение суда (решение о признании лица недееспособным или ограниченно дееспособным или о ликвидации юридического лица).

### §2. Выдача сертификата удостоверяющими центрами государственных органов

8. Для получения сертификата заявитель представляет в удостоверяющий центр государственных органов следующие документы:

-заявление для получения сертификата согласно приложению 4 настоящих Правил;

- копию паспорта (или иной документ, удостоверяющий личности) для физических лиц;

- копию свидетельства о регистрации в налоговом органе, копию учредительных документов и доверенность для юридических лиц;

9. Заявитель несет ответственность за предоставление достоверной информации.

10. Выдача сертификатов заявителю осуществляется одним из следующих способов:

- в режиме офлайн (при подаче заявления сотрудником оператора);

- в режиме онлайн (при подаче заявления заявителем);

- посредством системы «Имзо».

11. Выдача сертификатов заявителю, в режиме офлайн, осуществляется в следующих случаях:

-первичная выдача сертификата;

-в случае необходимости получения второго действующего сертификата (дубликат).

12. Удостоверяющий центр государственных органов выдает сертификат заявителю на основании заявления для получения сертификатов в режиме офлайн направленного посредством электронной почты.

13. Сотрудник оператора производит генерацию закрытого ключа защищенной электронной подписи и выпуск сертификата заявителю. Удостоверяющий центр государственных органов формирует открытый ключ в соответствии с утвержденным стандартом.

14. Ключ передается заявителю специальной почтовой связью или через ответственного сотрудника заявителя, в случае указания его фамилии, имени отчества в письме в качестве исполнителя, при предъявлении служебного удостоверения или доверенности на получение сертификата.

15. При получении сертификата ответственный сотрудник заявителя расписывается в журнале установленной формы согласно приложению 5 настоящих Правил.

16. Сотрудник оператора заносит сведения о сертификате в реестр удостоверяющего центра государственных органов.

17. Выдача сертификата заявителю, в режиме онлайн, осуществляется в следующих случаях:

-заявитель посредством сайта направляет в удостоверяющий центр государственных органов заявление на получение сертификата посредством сервиса подачи заявки онлайн согласно приложению 6 настоящих Правил.

-заявитель или система генерирует закрытый ключ, путем подачи заявки в сервисе подачи заявки онлайн удостоверяющий центр государственных органов посредством сайта.

18. Сотрудник оператора, после получения заявления на получение сертификата посредством сервиса подачи заявки онлайн от заявителя, осуществляет проверку предоставленных данных на полноту и подтверждает заявку на выдачу сертификатов.

19. Заявитель после подтверждения заявки сотрудником оператора, устанавливает сертификат.

20. Сотрудник оператора заносит сведения о сертификате в реестр удостоверяющего центра государственных органов.

21. Выдача сертификата заявителю, посредством системы «Имзо» осуществляется в следующих случаях:

-заявитель подает заявку посредством системы «Имзо»;

-обращения передается в удостоверяющий центр государственных органов после проверки биометрии (распознавание лица и отпечатки пальцев);

-система «Имзо» подписывает ключами защищенной электронной подписи заявку, которая направляется в удостоверяющий центр государственных органов;

- удостоверяющий центр государственных органов после получения заявки от системы «Имзо», выпускает сертификат.

22. Сертификат выдаётся в следующие сроки с момента получения заявления:

-для физических и юридических лиц – в течение пяти рабочих дней;

-для государственных служащих – в течении одного рабочего дня.

23. Сертификат для пользователей удостоверяющего центра выдается на алгоритме RSA или ГОСТ 34.10.2012-256.

24. Ответом на заявления по выпуску сертификата осуществляется следующим образом:

-для режима офлайн – передача заявителю нарочно или специальной почтовой связью;

-для режима онлайн и системы «Имзо» – выпуск сертификата для пользователя удостоверяющего центра.

25. Срок действия сертификата составляет один год с момента его выпуска и указывается в самом сертификате.

26. Удостоверяющие центры государственных органов обязаны вести реестр, который должен содержать следующую информацию:

-уникальный номер сертификата;

-данные пользователя;

-срок действия сертификата;

-историю внесения изменений или отзыва.

27. Удостоверяющие центры государственных органов отказывает в выдаче сертификата в следующих случаях:

1) предоставление недостоверной или неполной информации;

2) вступление в законную силу решение суда (решение о признании лица недееспособным или ограниченно дееспособным);

3) не достижения лицом шестнадцатилетнего возраста;

4) несоответствие заявителя требованиям законодательства;

5) наличия действующего сертификата у пользователя удостоверяющего центра, за исключением следующих случаев:

-одновременной работы пользователя в двух государственных органах (при наличии подтверждающих документов);

-пользователь с правом подписи запросов на выпуск сертификата для пользователей удостоверяющего центра государственных органов в системе «Имзо».

28. Ответ об отказе в выдаче сертификата заявителю должен содержать следующую информацию:

-для режима офлайн – письменный ответ предоставляется заявителю посредством электронной почты, в течение пяти рабочих дней со дня обращения заявителя в удостоверяющий центр государственных органов;

-для режима онлайн – путем отклонения заявки в сервисе подачи заявки онлайн с предоставлением причины отказа;

-для системы «Имзо» – путем отклонения заявки в сервисе подачи заявки онлайн, с предоставлением причины отказа.

29. Выдача сертификата со стороны удостоверяющего центра государственных органов для VPN устройства осуществляется следующим способом:

-заявитель посредством сайта направляет письмо на получение сертификата в уполномоченный орган;

-уполномоченный орган после проверки письма и положительного решения о необходимости выпуска сертификата для VPN устройства, отписывает письмо сотруднику оператора для его дальнейшего выпуска;

-сотрудник оператора, после получения письма от уполномоченного органа, осуществляет проверку предоставленных данных на его корректность, далее выпускает сертификат;

-сотрудник оператора передает сертификат для VPN устройств заявителю, посредством специальной почтовой связи либо нарочно.

30. Сертификат выдается в форме электронного документа со структурой, соответствующей приложениям 8 и 9 настоящих Правил.

## 3. ПОРЯДОК ХРАНЕНИЯ СЕРТИФИКАТА

### §1. Хранения сертификатов удостоверяющим центром, в частности корневым удостоверяющим центром

31. Срок хранения сертификата определяется соглашением, заключенным между удостоверяющим центром, в частности корневым удостоверяющим центром и пользователем сертификата.

32. По истечении указанного срока хранения сертификат исключается из реестра и переносится на архивное хранение. Хранение документов осуществляется с указанием срока хранения.

33. По истечении срока хранения отозванные сертификаты сдаются на архивное хранение в порядке, установленном законодательством Республики

Таджикистан. После истечения срока действия сертификата он удаляется из реестра и переносится в архив прекращенных сертификатов.

### §2. Хранение сертификатов со стороны удостоверяющих центров государственных органов

34. Хранение документов о создании и аннулировании защищенной электронной подписи осуществляется в порядке, установленном законодательством Республики Таджикистан.

35. По истечении установленного срока документы о создании и аннулировании защищенной электронной подписи сдаются на хранение в архив в порядке, установленном законодательством Республике Таджикистан.

36. Сертификаты хранятся в реестре удостоверяющих центров государственных органов. Они защищены от постороннего доступа и предоставляются заинтересованным лицам только в случае подтверждения их права на доступ.

37. Реестр должен иметь резервную копию, которая регулярно обновляется и хранится в защищенном месте. В случае компрометации или технического сбоя удостоверяющие центры государственных органов принимают соответствующие меры для восстановления данных из резервной копии.

38. По истечении одного года, документы о создании и аннулировании защищенной электронной подписи, поступают на архивное хранение.

39. Хранение ключей удостоверяющих центров государственных органов выполняются следующими способами:

-сертифицированных аппаратных и программных модулей безопасности;

-политика многопользовательского управления доступом (с использованием разделения полномочий);

- удостоверяющий центр государственных органов регулярно проводить проверку систем хранения ключей и принимает соответствующие меры по предотвращению угроз их компрометации.

40. Пользователь несет ответственность за утрату или компрометацию закрытого ключа в результате ненадлежащего хранения.

41. Удостоверяющие центры государственных органов несут ответственность за нарушение правил хранения сертификатов и ключевой информации в своем распоряжении.

42. В случае выявления нарушений безопасности стороны обязаны немедленно принять меры для их устранения.

## 4. ПОРЯДОК ОТЗЫВА СЕРТИФИКАТА

### §1. Отзыв сертификата удостоверяющего центра и отзыв сертификатов пользователей

43. Отзыв сертификата удостоверяющего центра со стороны корневого удостоверяющего центра осуществляется в следующих случаях.

- по требованию удостоверяющего центра, либо его представителя на основании заявления на отзыв сертификата согласно приложению 2 настоящих Правилам;

- при установлении факта представления недостоверных сведений либо неполного пакета документов при получении сертификата;

- смены наименования, реорганизации, ликвидации юридического лица – пользователя, смены руководителя юридического лица;

- в других случаях, предусмотренных законодательством Республики Таджикистан.

44. Для отзыва сертификата, удостоверяющий центр представляет в корневой удостоверяющий центр официальное письмо с подтверждающим документом наступления одного из случаев, предусмотренных пунктом 43 настоящих Правил.

45. Отзыв сертификата удостоверяющего центра осуществляется в течение трех дней.

46. После рассмотрения документов и отзыва сертификата корневой удостоверяющий центр вносит записи в реестр о прекращении действия сертификата с указанием даты, причины и времени отзыва сертификата удостоверяющего центра в течении одного рабочего дня со дня получения соответствующей информации.

47. Корневой удостоверяющий центр публикует сведения об отозванных сертификатах, их уникальные номера и причину отзыва на своём официальном сайте. Обновление реестра производится с периодичностью не менее одного раза в день.

48. Удостоверяющий центр, в частности корневой удостоверяющий центр выдавший сертификат пользователям, отзывает его на основании соответствующего уведомления в следующих случаях:

- по требованию пользователя или его законного представителя;

- при определении факта предоставления неверной информации или неполного пакета документов при получении сертификата;

- смерть пользователя;

- изменение фамилии, имени или отчества (если это указано в документе, удостоверяющем личность) пользователя (для физических лиц);

- изменение наименования, реорганизация или ликвидация юридического лица - пользователя или смена руководителя юридического лица;

- вступление в законную силу решение суда (решение о признании лица недееспособным или ограниченно дееспособным или о ликвидации юридического лица);

- другие обстоятельства, предусмотренные соглашением между удостоверяющим центром, в частности корневой удостоверяющий центром и пользователем.

49. Для отзыва сертификата пользователь или другие законные заинтересованные лица обращаются в удостоверяющий центр, в частности корневой удостоверяющий центр в электронной форме или через

информационную систему в случае возникновения одного из обстоятельств, указанных в пункте 48.

50. Отзыв сертификата пользователей со стороны удостоверяющего центра, в частности корневого удостоверяющего центра осуществляется в течение одного рабочего дня.

51. После отзыва в реестр поступает соответствующая запись о прекращении действия сертификата с указанием даты, причины и времени отзыва сертификата.

52. Удостоверяющий центр, в частности корневой удостоверяющий центр публикует информацию об отзываемых сертификатах, их уникальных номерах и причинах отзыва в реестре отзываемых сертификатов на своем официальном сайте.

53. Реестр отозванных сертификатов пересматривается не реже одного раза в месяц.

## §2. Отзыв сертификатов пользователей со стороны удостоверяющих центров государственных органов

54. Удостоверяющие центры государственных органов отзывает сертификат пользователя в следующих случаях:

-по требованию пользователя сертификата или его представителя на основании заявления на отзыв сертификата пользователя по форме согласно приложению 7 настоящих Правил;

-при установлении факта представления недостоверных сведений либо неполного пакета документов при получении сертификата;

-смерти пользователя;

-изменения фамилии, имени или отчества (если оно указано в документе, удостоверяющем личность) пользователя;

-смены наименования, реорганизации, ликвидации юридического лица – пользователя, смены руководителя юридического лица;

-на основании решения уполномоченного государственного органа;

- вступление в законную силу решение суда (решение о признании лица недееспособным или ограниченно дееспособным или о ликвидации юридического лица);

- другие обстоятельства, предусмотренные соглашением между удостоверяющими центрами государственных органов и пользователями.

55. Отзыв сертификата пользователей осуществляется одним из следующих способов:

-в режиме офлайн (при подаче заявления сотрудником оператора);

-в режиме онлайн (при подаче заявления заявителем);

-посредством системы «Имзо».

56. Отзыв сертификата пользователей в режиме офлайн осуществляется сотрудником оператора на основании заявления на отзыв.

57. Отзыв сертификата пользователей в режиме онлайн осуществляется следующим образом:

-заявитель отправляет запрос на отзыв сертификата путем подачи заявки в системе подачи заявки онлайн;

-заявитель направляет в удостоверяющий центр заявку на отзыв;

-сотрудник оператора, после получения письма заявителя, осуществляет проверку предоставленных данных на полноту и подтверждает запрос на отзыв сертификата.

58. Отзыв сертификатов пользователей посредством системы «Имзо» осуществляется таким образом:

-заявитель подает заявку посредством системы «Имзо»;

-заявка подписывается ключами защищенной электронной подписи заявителя и направляется в систему «Имзо»;

- удостоверяющий центр после получения заявки от системы «Имзо», отзывает сертификат пользователя.

59. Удостоверяющие центры государственных органов обязаны рассмотреть заявление на отзыв сертификата в срок, не превышающий 3 рабочих дней с момента ее получения. При рассмотрении заявление удостоверяющий центр государственных органов проверяет правомерность оснований для отзыва, определяет личность заявителя и проводит дополнительные проверки.

60. Удостоверяющие центры государственных органов исключают сертификат пользователя из реестра, опубликовывают сведения об отозванных сертификатах, их уникальные номера и причину отзыва и уведомляют пользователей и заинтересованные стороны.

61. Обновление реестра отозванных сертификатов осуществляется незамедлительно и публикуется в открытом доступе на официальном сайте.

## 5. ПОРЯДОК ПОДТВЕРЖДЕНИЯ ПРИНАДЛЕЖНОСТИ И ДЕЙСТВИТЕЛЬНОСТИ ОТКРЫТОГО КЛЮЧА ЗАЩИЩЕННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

62. При отправке электронного документа с сертификатом соответствующая информационная система выполняет проверку принадлежности и действительности открытого ключа защищенной электронной подписи следующим образом:

- проверка защищенной электронной подписи в электронном документе;

- проверка сертификата подписавшей стороны.

63. Соответствующая информационная система проверяет наличие защищенной электронной подписи в электронном документе с помощью открытого ключа электронной подписи, содержащегося в сертификате подписавшей стороны. Электронный документ должен содержать сертификат подписавшей стороны.

64. Для подтверждения принадлежности открытого ключа защищенной электронной подписи удостоверяющие центры, в частности, корневой удостоверяющий центр и удостоверяющие центры государственных органов выполняют следующие действия:

-проверяют сведения о пользователе в реестре;

-сопоставляют указанные в запросе данные с информацией в сертификате;

-если информация совпадает, удостоверяющий центр подтверждает принадлежность сертификата пользователю;

-в случае расхождений удостоверяющий центр уведомляет заявителя о невозможности подтверждения принадлежности ключа.

65. Для подтверждения действительности сертификата удостоверяющие центры, в частности корневой удостоверяющий центр и удостоверяющие центры государственных органов выполняют следующие действия:

-проверяют наличие сертификата в реестре;

-убеждаются в отсутствии сертификата в реестре отозванных сертификатов;

-проверяют срок действия сертификата;

-если сертификат действителен, удостоверяющий центр государственных органов подтверждает его статус заявителю;

-в случае обнаружения, что сертификат недействителен (истек срок действия или он отозван), удостоверяющие центры государственных органов информируют об этом заявителя.

66. Удостоверяющие центры, в частности корневой удостоверяющий центр и удостоверяющие центры государственных органов обязаны обеспечивать доступность информации о действительных и отозванных сертификатах на своём официальном сайте.

## 6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

67. За несоблюдение положений настоящих Правил ответственные лица привлекаются к ответственности в соответствии с законодательством Республики Таджикистан.

ВАЗОРАТИ АДЛИЯИ
ҶУМҲУРИИ ТОҶИКИСТОН
ФЕҲРИСТИ БАҲИСОБГИРИИ ДАВЛАТИИ
САНАДҲОИ МЕЪЁРИИ ҲУҚУҚИИ
ҶУМҲУРИИ ТОҶИКИСТОН
БА ҚАЙД ГИРИФТА ШУД
Р/Б № 1329
"28" 02 с.20 25

Приложение 1
к Правилам выдачи, хранения, отзыва сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в частности корневым удостоверяющим центром и удостоверяющими центрами государственных органов

## Заявление для получения сертификата

Настоящим я, _____

(фамилия, имя, отчество (при его наличии) представителя, дата рождения)

Идентификационный номер налогоплательщика представителя: _____

(наименование юридического лица, адрес, телефон)

прошу обработать запрос регистрации удостоверяющего центра (PKCS#10) в формате Base64: _____

(тело запроса)

и изготовить сертификат удостоверяющего центра в соответствии с указанными в заявлении сведениями.

Идентификационные данные: _____

Наименование страны: _____

Наименование области: _____,

город _____

Наименование организации: _____

Наименование удостоверяющего центра: _____

Адрес электронной почты: _____

Область использования сертификата: _____

Дата «____» _____ 20___ год.

Руководитель (начальник) _____

(подпись, фамилия, имя, отчество) М.П

ВАЗОРАТИ АДЛИЯИ
ҶУМҲУРИИ ТОҶИКИСТОН
ФЕҲРИСТИ БАҲИСОБГИРИИ ДАВЛАТИИ
САНАДҲОИ МЕЪЁРИИ ҲУҚУҚИИ
ҶУМҲУРИИ ТОҶИКИСТОН
БА ҚАЙД ГИРИФТА ШУД
Р/Б № 1328
«28» 02 с.20 25

Приложение 2
к Правилам выдачи, хранения, отзыва сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в частности корневым удостоверяющим центром и удостоверяющими центрами государственных органов

## Заявление на отзыв сертификата

Настоящим я, _____

_____

(фамилия, имя, отчество представителя, дата рождения)

Идентификационный номер налогоплательщика представителя: _____

_____

(наименование юридического лица, адрес, телефон)

прошу отозвать ранее выданный сертификат удостоверяющего центра в связи с: _____

_____

_____

Серийный номер сертификата: _____

Наименование страны: _____

Наименование области: _____,

город _____

Наименование организации: _____

Наименование удостоверяющего центра: _____

_____

Адрес электронной почты: _____

Срок действия сертификата: _____

_____

Дата «____» _____ 20___ год.

Руководитель (начальник) _____

(подпись, фамилия, имя, отчество) М.П

ВАЗОРАТИ АДЛИЯИ
ҶУМҲУРИИ ТОҶИКИСТОН
ФЕҲРИСТИ БАҲИСОБГИРИИ ДАВЛАТИИ
САНАДҲОИ МЕЪЁРИИ ҲУҚУҚИИ
ҶУМҲУРИИ ТОҶИКИСТОН
БА ҚАЙД ГИРИФТА ШУД
Р/Б № 1329
"28" 02 с.2025

Приложение 3
к Правилам выдачи, хранения, отзыва сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в частности корневым удостоверяющим центром и удостоверяющими центрами государственных органов

План
оказания услуг по выдаче сертификата

| Этапы | Субъекты | Мероприятия | Сроки исполнения |
|---|---|---|---|
| 1-й этап | Заявитель | 1. Электронное или явочное обращение в центр государственных услуг за получением сертификата ключа защищенной электронной подписи.<br>2. Оплата сборов за оказание государственных услуг. | 1. По желанию<br>2. При обращении |
| 2-й этап | Центр государственных услуг | 1. Заполнение анкеты от имени заявителя и отправление ее в уполномоченный орган.<br>2. Направление запроса в уполномоченный орган. | 1. В течение 20 минут<br>2. Автоматически |
| 3-й этап | Уполномоченный орган | 1. Рассмотрение представленной информации.<br>2. Регистрация ключей защищенной электронной подписи и подготовка сертификата ключа электронного цифрового подписа или уведомления об отказе.<br>3. Внесение сертификата ключа защищенной электронной подписи в реестр, и отправка кода ключа электронной цифровой подписи заявителю в виде QR-кода | Автоматически |

| | | | |
|---|---|---|---|
| | | 4. Отправка оформленного сертификата ключа защищенной электронной подписи или уведомления об отказе по обоснованным причинам в центр государственных услуг. | |
| 4-й этап | Центр государственных услуг | 1. Получение от уполномоченного органа сертификата ключа защищенной электронной подписи или уведомления об отказе по обоснованным причинам.<br><br>2. Идентификация владельца закрытого ключа защищенной электронной подписи, запись ключей ключа электронного цифрового подписа и сертификата ключа защищенной электронной подписи на внешний носитель информации.<br><br>3. Оформление сертификата ключа защищенной электронной подписи в электронном виде или QR кодом и выдача закрытого ключа защищенной электронной подписи владельцу либо отказ по обоснованным причинам. | В течение 20 минут |

Приложение 4
к Правилам выдачи, хранения, отзыва сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в частности корневым удостоверяющим центром и удостоверяющими центрами государственных органов

Заявление для получения сертификатов

С уважением просим Вас помочь о содействии в получении сертификата следующим сотрудникам:

| № | Фамилия, имя, отчество | Идентификационный номер налогоплательщика (организации) | Организация | Должность | Область, город, район | Адрес электронной почты (для оповещения об истечении срока действий) | Абонентский номер сотовой связи |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 4 | 5 | 6 | 7 | 8 | 9 |
| | | | | | | | |

Руководитель (начальник) _____ _____
(подпись) М.П. Фамилия, имя, отчество

Исполнитель
Фамилия, имя, отчество: _____
Телефон: _____

ВАЗОРАТИ АДЛИЯИ
ҶУМҲУРИИ ТОҶИКИСТОН
ФЕҲРИСТИ БАҲИСОБГИРИИ ДАВЛАТИИ
САНАДҲОИ МЕЪЁРИИ ҲУҚУҚИИ
ҶУМҲУРИИ ТОҶИКИСТОН
БА ҚАЙД ГИРИФТА ШУД
Р/Б № 1328
«28» 02 с.20 25

Приложение 5
к Правилам выдачи, хранения, отзыва сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в частности корневым удостоверяющим центром и удостоверяющими центрами государственных органов

Журнал учета выдачи сертификатов пользователям

| № | Наименование государственного органа | Номер и дата письма | Фамилия, имя, отчество пользователя, на которого выпущено сертификат | Дата выпуска сертификата | Серийный номер | Фамилия, имя, отчество получателя | Подпись | Дата |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

ВАЗОРАТИ АДЛИЯИ
ҶУМҲУРИИ ТОҶИКИСТОН
ФЕҲРИСТИ БАҲИСОБГИРИИ ДАВЛАТИИ
САНАДҲОИ МЕЪЁРИИ ҲУҚУҚИИ
ҶУМҲУРИИ ТОҶИКИСТОН
БА ҚАЙД ГИРИФТА ШУД
Р/Б № 1329
"28" 02 с. 25

Приложение 6
к Правилам выдачи, хранения, отзыва сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в частности корневым удостоверяющим центром и удостоверяющими центрами государственных органов

Заявление на получение сертификатов посредством сервиса подачи заявки онлайн

С уважением просим Вас помочь в выдаче сертификата следующим сотрудникам:

| № | Фамилия, имя, отчество | Идентификационный номер налогоплательщика | Организация | Должность | Область, город, район | Номер заявки (заполняется при подаче онлайн) | Адрес электронной почты (для оповещения об истечении срока действий) | Абонентский номер сотовой связи |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | | | | | | | | |

Руководитель (начальник) _____ _____
(подпись) М.П. Фамилия, имя, отчество

Исполнитель
Фамилия, имя, отчество: _____
Телефон: _____

ВАЗОРАТИ АДЛИЯИ
ҶУМҲУРИИ ТОҶИКИСТОН
ФЕҲРИСТИ БАҲИСОБГИРИИ ДАВЛАТИИ
САНАДҲОИ МЕЪЁРИИ ҲУҚУҚИИ
ҶУМҲУРИИ ТОҶИКИСТОН
БА ҚАЙД ГИРИФТА ШУД
Р/Б № 1328
"28" 02 с.2025

Приложение 7
к Правилам выдачи, хранения, отзыва сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в частности корневым удостоверяющим центром и удостоверяющими центрами государственных органов

Заявление на отзыв сертификата пользователей удостоверяющих центров государственных органов

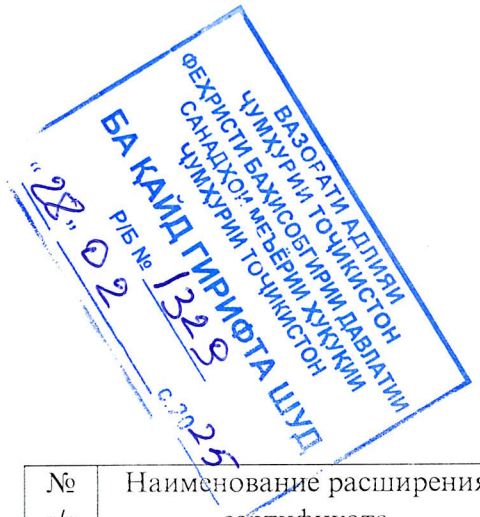
С уважением просим Вас отозвать сертификаты следующих сотрудников:

| № | Фамилия, имя, отчество | Идентификатционный номер налогоплательщика | Идентификатционный номер налогоплательщика (организации) | Организация |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |

Руководитель (начальник) _____ _____
(подпись) М.П. Фамилия, имя, отчество

Исполнитель
Фамилия, имя, отчество: _____
Телефон: _____

ВАЗОРАТИ АДЛИЯИ
ҶУМҲУРИИ ТОҶИКИСТОН
ФЕҲРИСТИ БАҲИСОБГИРИИ ДАВЛАТИИ
САНАДҲОИ МЕЪЁРИИ ҲУҚУҚИИ
ҶУМҲУРИИ ТОҶИКИСТОН
БА ҚАЙД ГИРИФТА ШУД
Р/Б № 1329
"28" 02 с.2025




Приложение 8
к Правилам выдачи, хранения, отзыва сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в
частности корневым удостоверяющим центром и удостоверяющими центрами государственных органов

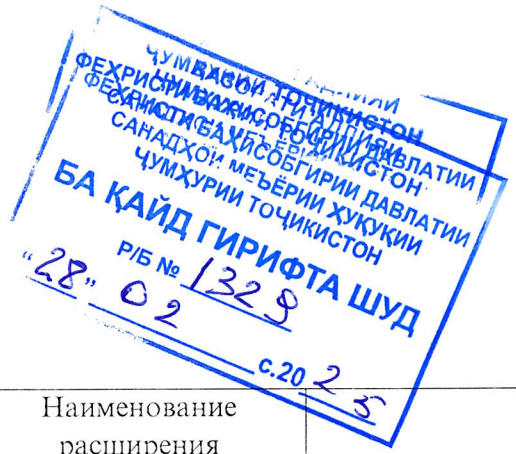
Структура сертификата пользователей

| № п/н | Наименование расширения сертификата | Определение | Содержание |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1. Базовые расширения сертификатов в формате X.509 | | | |
| 1) | Version | В данном расширении указывается версия | V3 |
| 2) | Serial Number | Расширение, определяющее уникальный серийный номер каждого сертификата, выпущенного определенным удостоверяющим центром | Целое число в шестнадцатеричном представлении длиной 32 байта |
| 3) | Signature | Содержит идентификатор алгоритма для алгоритма и хэш-функции, используемой удостоверяющим центром при подписании сертификата | Значение |
| 4) | Issuer | Определяет идентификационное имя удостоверяющего центра, подписавшего и издавшего данный сертификат | Значение |
| 5) | Validity | Определяет интервал времени, в течение которого удостоверяющий центр гарантирует, что он будет поддерживать информацию о статусе сертификата | Действителен с: YYYYMMDDHHMMSSZ GMT<br>Действителен по: YYYYMMDDHHMMSSZ GMT |
| 6) | Subject | Определяет объект, связанный с открытым ключом, содержащимся в поле открытого ключа субъекта | Значение |
| 2. Дополнительные расширения сертификатов | | | |
| 1) | SubjectPublicKeyInfo | Расширение, используемое для хранения открытого ключа и для определения алгоритма, примером, которого является данный открытый ключ | Значение |
| 2) | Extensions | Делает возможным добавление новых полей в структуру без изменения определения ASN.1. | Значение |

| | | | |
|---|---|---|---|
| 3) | AthorityInfoAccess | Расширение, используемое для хранения информации о сервисах удостоверяющего центра, в том числе Online Certificate Status Protocol (OCSP) любых форматов | Значение |
| 4) | AthorityKeyIdentifier | Идентификатор ключа уполномоченного лица удостоверяющего центра | Значение |
| 5) | SubectKeyIdentifier | Идентификатор ключа владельца сертификата | Значение |
| 6) | KeyUsage | Назначение сертификата DigitalSignature – цифровая подпись, аутентификация<br>onrepudiation – цифровая подпись;<br>keyEncipherment – аутентификация. | Цифровая электронная подпись, Неотрекаемость (c0) |
| 7) | ExtendedKeyUsage | Область использования сертификата, при которых электронный документ с электронной защищенной подписью (электронной цифровой подписью) будет иметь юридическое значение. Возможные значения:<br>- Client Authentication<br>- emailProtection | Значение |
| 8) | CRL Distribution Points | Точка распространения реестра отозванных сертификатов | Значение |
| 9) | CertificatePolicies | Политика сертификатов | Значение |
| 10) | SubjectAltName | Расширение определяет дополнительные субъекты распространяемый действием данного сертификата | Значение |

Требования к идентификационным данным сертификата физического и юридического лица

| № п/н | Наименование полей | Значение | Примечание |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1. Обязательные значения для полей | | | |
| 1) | Country | TJ | Указывается наименование страны, резидентом которой является владелец сертификата |
| 2) | Organization | Наименование организации | Значение поля – полное наименование организации (без сокращений), даже если оно превышает 256 символов. Возможно удаление или замена специальных непечатных символов, если возникают проблемы с выпуском сертификатов. |
| 2. Рекомендуемые значения для полей | | | |
| 1) | Organization unit | Идентификационный номер налогоплательщика | Данное поле является не уникальным, и в одном сертификате может быть несколько полей «OU». |
| 2) | Serial number | Единый номер | Значение |




Приложение 9
к Правилам выдачи, хранения, отзыва сертификатов и подтверждение принадлежности и действительности открытого ключа защищенной электронной подписи удостоверяющим центром, в частности корневым удостоверяющим центром, удостоверяющими центрами государственных органов

Структура сертификата удостоверяющего центра

| № п/н | Наименование расширения сертификата | Определение | Содержание |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1. Базовые расширения сертификата в формате X.509 | | | |
| 1) | Version | В данном расширении указывается версия (X.509v3) | V3 |
| 2) | Serial Number | Расширение, определяющее уникальный серийный номер каждого сертификата, выпущенного определенным удостоверяющим центром | Целое число в шестнадцатеричном представлении длиной 32 байта |
| 3) | Signature | Содержит идентификатор алгоритма для алгоритма и хэш-функции, используемой удостоверяющим центром при подписании сертификата | Значение |
| 4) | Issuer | Определяет DN удостоверяющего центра, подписавшего и издавшего данный сертификат | Значение |
| 5) | Validity | Определяет интервал времени, в течение которого удостоверяющий центр гарантирует, что он будет поддерживать информацию о статусе сертификата | Действителен с: YYYYMMDDHHMMSSZ GMT<br>Действителен по: YYYYMMDDHHMMSSZ GMT |
| 6) | Subject | Определяет объект, связанный с открытым ключом, содержащимся в поле открытого ключа субъекта | Значение |
| 2. Дополнительные расширения сертификатов | | | |
| 1) | SubjectPublicKeyInfo | Расширение, используемое для хранения открытого ключа и для определения алгоритма, примером, которого является данный открытый ключ | Значение |

| | | | |
|---|---|---|---|
| 2) | Extensions | Делает возможным добавление новых полей в структуру без изменения определения ASN.1. | Значение |
| 3) | SubectKeyIdentifier | Идентификатор ключа владельца сертификата | Значение |
| 4) | KeyUsage | Назначение сертификата. Содержит следующие значения:<br>CRLSign – определяется политика корневого сертификата удостоверяющего центра (опциональное значение)<br>KeyCertSgin –указывает на сертификат удостоверяющего центра | Значение |
| 5) | ExtendedKeyUsage | Область использования ключа, при которых электронный документ с электронной защищенной подписью (электронной цифровой подписью) будет иметь юридическое значение. Возможные опциональные значения:<br>- Time stamping<br>- OCSPSigning | Значение |
| 6) | Basic constraints | Тип субъекта. Значение cA = True | Значение |
| 7) | SubjectAltName | Расширение определяет дополнительные субъекты распространяемый действием данного сертификата | Значение |

Требования к идентификационным данным сертификата удостоверяющего центра

| № п/н | Наименование полей | Значение | Примечание |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1. Обязательные значения для полей | | | |
| 1) | Country | TJ | Значение поля всегда равно «TJ» |
| 2) | Organization | Наименование организации | Значение поля – полное наименование организации (без сокращений), даже если оно превышает 256 символов. Возможно удаление или замена специальных непечатных символов, если возникают проблемы с выпуском сертификатов. |
| 2. Рекомендуемые значения для полей | | | |
| 1) | Organization unit | Бизнес идентификационный номер | Данное поле является не уникальным и в одном сертификат может быть несколько полей «OU». |

ВАЗОРАТИ АДЛИЯИ
ҶУМҲУРИИ ТОҶИКИСТОН
ФЕҲРИСТИ БАҲИСОБГИРИИ ДАВЛАТИИ
САНАДҲОИ МЕЪЁРИИ ҲУҚУҚИИ
ҶУМҲУРИИ ТОҶИКИСТОН
БА ҚАЙД ГИРИФТА ШУД
Р/Б № 1329
28" 02 с.2025