

ТРЕБОВАНИЯ
к средствам электронной подписи и
к средствам удостоверяющего центра

Глава 1. Общие положения

1. Настоящие Требования к средствам электронной подписи и к средствам удостоверяющего центра (далее – Требования) предназначены для подтверждения соответствия используемых юридическими лицами или индивидуальными предпринимателями средств электронной подписи и средств удостоверяющего центра нормативным правовым актам Кыргызской Республики.

2. Настоящие Требования не распространяются на средства защиты сведений, относящиеся к государственным секретам Кыргызской Республики.

3. Настоящие Требования разработаны в соответствии с Законом Кыргызской Республики «Об электронной подписи» (далее – Закон) и во исполнение пункта 2 постановления Правительства Кыргызской Республики «О некоторых вопросах, связанных с использованием электронной подписи» от 31 декабря 2019 года № 742.

4. Настоящие Требования распространяются на средства электронной подписи и средства удостоверяющего центра, используемые на территории Кыргызской Республики юридическими лицами или индивидуальными предпринимателями.

5. В настоящих Требованиях используются основные понятия, указанного Закона:

- электронная подпись (далее – ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме и (или) логически связана с ней и которая используется для определения лица, от имени которого подписана информация;

- удостоверяющий центр (далее – УЦ) - юридическое лицо или индивидуальный предприниматель, осуществляющие деятельность по созданию и выдаче сертификатов ключа проверки подписи;

- ключ подписи - уникальная последовательность символов, предназначенная для создания ЭП;

- ключ проверки подписи - уникальная последовательность символов, однозначно связанная с ключом подписи и предназначенная для проверки подлинности ЭП (далее – проверка ЭП);

- средства ЭП - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание ЭП, проверка ЭП, создание ключей ЭП и ключей проверки ЭП;
- сертификат ключа проверки ЭП - электронный документ или документ на бумажном носителе, выданный УЦ и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП;
- владелец сертификата ключа проверки ЭП - лицо, которому в порядке, установленном указанным Законом, удостоверяющим центром выдан сертификат ключа проверки подписи;
- средства УЦ - программные и (или) аппаратные средства, используемые для реализации функций создания, хранения и выдачи сертификатов ключа проверки подписи, а также ведения реестра сертификатов ключа проверки подписи;
- участники электронного взаимодействия - государственные органы, органы местного самоуправления, организации и учреждения, а также граждане, обменивающиеся информацией в электронной форме.

Глава 2. Требования к средствам электронной подписи

6. Средства ЭП могут быть реализованы с использованием аппаратных и программных средств.
7. При создании электронной подписи средства ЭП должны:
 - показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;
 - создавать ЭП лишь после подтверждения лицом, подписывающим информацию, операции по созданию ЭП;
 - однозначно и ясно показывать, что ЭП создана.
8. При проверке ЭП средства ЭП должны:
 - показывать содержание электронного документа, подписанного ЭП;
 - показывать вносились ли изменения в подписанный ЭП электронный документ;
 - указывать на лицо, с использованием ключа ЭП которого подписаны электронные документы.
9. Средства ЭП должны обеспечивать практическую невозможность вычисления ключа подписи из электронной подписи или из ключа ее проверки.
10. Средства ЭП должны противостоять угрозам, представляющим собой целенаправленные действия с использованием аппаратных и (или) программных средств, с целью нарушения безопасности, защищаемой средством ЭП информации, или с целью создания условий для этого.
11. Средства электронной подписи, предназначенные для создания электронной подписи в электронных документах, содержащих

конфиденциальную информацию, не должны нарушать конфиденциальности такой информации.

12. Соответствие средств ЭП настоящим требованиям, может подтверждаться соответствующими официальными сертификатами, которые признаны на территории Кыргызской Республики.

Глава 3. Требования к средствам удостоверяющего центра

13. Средства УЦ должны противостоять угрозам, определяемых как целенаправленные действия с применением аппаратных и (или) программных средств, направленных на нарушение инженерной, технической, программной и криптографической безопасности средств УЦ или с целью создания условий для этого.

14. Средства УЦ должны применяться в условиях, отвечающих Требованиям к защите информации, содержащейся в базах данных государственных информационных систем, утвержденным постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 762 (далее – Требования по ЗИ).

15. Средства УЦ, участвующие в обработке персональных данных, должны соответствовать Требованиям к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных, утвержденным постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 760 (далее – Требования по безопасности ПД).

16. Протоколы создания и аннулирования сертификатов ключей проверки ЭП должны быть отражены в регламенте УЦ.

17. Средства УЦ должны реализовывать протокол аннулирования сертификата ключа проверки ЭП с использованием списков аннулированных сертификатов.

18. Допускается реализация протоколов аннулирования без использования списков аннулированных сертификатов, требования к которым должны быть указаны в техническом задании на разработку или модернизацию средств УЦ.

19. В средствах УЦ должна быть реализована функция изготовления сертификата ключа проверки ЭП на бумажном носителе. Порядок выдачи сертификата ключа проверки ЭП на бумажном носителе и процедура проверки соответствия сертификата ключа проверки ЭП в электронном виде и на бумажном носителе должны быть отражены в документации средства УЦ.

20. В средствах УЦ в отношении владельца сертификата ключа проверки ЭП должны быть реализованы механизмы проверки уникальности ключа проверки ЭП и обладания соответствующим ключом ЭП.

21. Допустимые структуры сертификата ключа проверки ЭП и списка аннулированных сертификатов должны быть перечислены в эксплуатационной документации на средства УЦ.

22. В средствах УЦ должен быть реализован механизм контроля соответствия создаваемых сертификатов ключей проверки ЭП и списков аннулированных сертификатов заданной структуре.

23. В средствах УЦ должны быть реализованы механизмы хранения и поиска всех созданных сертификатов ключей проверки ЭП и списков аннулированных сертификатов в реестре, а также сетевого доступа к реестру.

24. В средствах УЦ должен быть реализован механизм поиска сертификатов ключей проверки ЭП и списков аннулированных сертификатов в реестре сертификатов ключей проверки ЭП по различным их атрибутам.

25. Все изменения реестра сертификатов ключей проверки ЭП должны регистрироваться в журнале аудита.

26. В эксплуатационной документации на средства УЦ должен быть описан механизм проверки подписи в сертификате ключа проверки ЭП по запросу участника электронного взаимодействия.

27. В средствах УЦ должен быть реализован механизм проверки подлинности ЭП УЦ в выдаваемых им сертификатах ключей проверки ЭП.

28. Проверка ЭП в сертификате ключа проверки ЭП осуществляется в соответствии с рекомендациями X.509, включая обязательную проверку всех критических дополнений.

29. Для ограничения возможностей атак на средства УЦ с использованием каналов связи должны применяться средства межсетевого экранирования.

30. Должны быть определены требования по защите средств УЦ от компьютерных вирусов.

31. Соответствие средств УЦ настоящим Требованиям, может подтверждаться соответствующими официальными сертификатами, которые признаны на территории Кыргызской Республики.