Приложение 2

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.

6^1. При создании ключей ЭП алгоритм создания ключа ЭП и ключа проверки ЭП должен обеспечивать криптографическую стойкость, исключать возможность практической реализации вычислительно эффективных атак, а также средства ЭП должны:

− обеспечить невозможность получения несанкционированного доступа к ключам ЭП, после их создания;

− защищать ключи ЭП и ключи проверки ЭП от искажения при его хранении;

− обеспечить доступность выполнения операций создания ЭП для владельца ключа ЭП.

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 ЭП 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 ЭП, предназначенные для создания электронной подписи в электронных документах, содержащих конфиденциальную информацию, не должны нарушать конфиденциальности такой информации.

11^1. Средство ЭП должно проводить аутентификацию владельца ключа подписи, осуществляющего локальный доступ к ключу подписи, используемому для выполнения подписи информации.

12. Средства ЭП должны иметь сертификат соответствия, выдаваемый уполномоченным государственным органом в сфере обеспечения национальной безопасности 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. Протоколы создания и аннулирования сертификатов ключей проверки ЭП должны быть отражены в регламенте УЦ.

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

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

17. 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.

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

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

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

21. 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.

22. 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.

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

23^{1}. Базовая операционная система средств УЦ должна поддерживать ведение журнала аудита системных событий.

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

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

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

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

28. Средства УЦ должны поддерживать ролевое разграничение членов группы администраторов средств УЦ. Должен быть определен список ролей и распределение обязанностей между ролями. Список ролей и распределение обязанностей между ролями должны быть указаны в регламенте УЦ.

29. Средства УЦ должны содержать механизм контроля несанкционированного случайного и (или) преднамеренного искажения (изменения, модификации) и (или) разрушения информации, программных средств и АС (далее АС – аппаратные средства) УЦ (далее – механизм контроля целостности), требования к которым должны быть указаны в техническом задании на разработку или модернизацию средств УЦ.

30. Должен быть определен период контроля целостности программных средств и АС УЦ, период должен быть указан в регламенте УЦ.

31. Должны иметься средства восстановления целостности средств УЦ.

32. Вероятность ошибки контроля целостности не должна превышать аналогичной вероятности для используемых средств криптографической защиты информации.

33. Средства УЦ должны обеспечивать управление доступом, требования к которым должны быть указаны в техническом задании на разработку или модернизацию средств УЦ

34. Ролевая модель средства УЦ должна предполагать наличие группы администраторов, операторов и пользователей. Группа администраторов должна обладать полным доступом к функционалу и настройки средства.

35. Идентификация и аутентификация включают в себя распознавание пользователя средств УЦ, оператора средства УЦ, члена группы администраторов средств УЦ и проверку их подлинности.

36. Аутентификация оператора и члена группы администраторов средства УЦ должна быть с применением криптографических методов и с использованием закрытого ключа на не извлекаемом ключевом носителе.

37. Описание процедуры регистрации пользователей средств УЦ (внесения данных в реестр пользователей средств УЦ) должно содержаться в эксплуатационной документации на средства УЦ.

38. Средства УЦ должны обеспечивать доверенный ввод самоподписанного сертификата ключа проверки ЭП.

39. Средства УЦ должны обеспечивать передачу данных, содержащих информацию ограниченного доступа, поступающих в УЦ и экспортируемых из УЦ, способом, защищенным от несанкционированного доступа.

40. В средствах УЦ должна быть реализована процедура защиты от навязывания ложных сообщений, требования к которым должны быть указаны в техническом задании на разработку или модернизацию средств УЦ.

41. Должны быть определены требования по надежности и устойчивости функционирования средств УЦ, требования к которым должны быть указаны в техническом задании на разработку или модернизацию средств УЦ.

42. Должен проводится расчет вероятности сбоев и неисправностей АС УЦ, приводящих к невыполнению УЦ своих функций.

43. Порядок создания, использования, хранения и уничтожения ключевой информации определяется в соответствии с требованиями эксплуатационной документации на средства ЭП и иные средства криптографической защиты информации, используемые средствами УЦ.

44. Срок действия ключа ЭП средства ЭП, используемого средствами УЦ, должен соответствовать требованиям, установленным к средствам ЭП.

45. Ключи ЭП, используемые для подписи сертификатов ключей проверки ЭП и списков уникальных номеров сертификатов ключей проверки ЭП, действие которых на определенный момент было прекращено УЦ до истечения срока их действия (далее – список аннулированных сертификатов), а

также ключи ЭП, используемые для подписи меток доверенного времени не должны использоваться ни для каких иных целей.

46. Сроки действия всех ключей должны быть указаны в эксплуатационной документации на средства УЦ.

47. Создаваемые УЦ сертификаты ключей проверки ЭП и списки аннулированных сертификатов должны соответствовать международным рекомендациям X.509. Все поля и дополнения, включаемые в сертификат ключей проверки ЭП и список аннулированных сертификатов, должны быть заполнены в соответствии с рекомендациями X.509. При использовании альтернативных форматов сертификатов ключей проверки ЭП должны быть определены требования к протоколам создания и аннулирования сертификатов ключей проверки ЭП и указаны в техническом задании на разработку или модернизацию средств УЦ.

48. Средство УЦ должно предоставлять пользователям возможность подачи заявок на выпуск сертификатов ключей проверки ЭП. Должна быть возможность ручной обработки заявки на сертификат оператором или членом группы администраторов средства УЦ в соответствии с регламентом УЦ. Должна быть возможность автоматической обработки заявки на сертификат в соответствии с регламентом средства УЦ.

49. Средство УЦ должно иметь возможность подключения к внешней ресурсной системе для извлечения сведений о пользователях и формирования на их основе сертификатов ключа проверки ЭП.

50. Средства ЭП должны иметь сертификат соответствия, выдаваемый уполномоченным государственным органом в сфере обеспечения национальной безопасности Кыргызской Республики.