Утвержден
приказом ГНС при ПКР
№____ от «_»_____2016 г.

РЕГЛАМЕНТ
взаимодействия Государственной налоговой службы при Правительстве Кыргызской Республики и специализированного оператора сервиса при представлении налоговой отчетности с применением электронной цифровой подписи посредством Системы электронной отчетности

Глава 1. Общие положения

Настоящий Регламент разработан на основании Закона Кыргызской Республики «Об электронном документе и электронной цифровой подписи» от 17 июля 2004 года N 92 и Налогового кодекса Кыргызской Республики от 17 октября 2008 года № 230 и определяет общие принципы организации информационного обмена при представлении налогоплательщиками налоговой отчетности в электронном виде через Систему электронной отчетности.

Цель и задача Системы информационного взаимодействия при представлении налоговой отчетности в электронном виде - сокращение контактов налогоплательщиков с органами налоговой службы.

1. Участники Системы признают, что применение в Системе средств ЭЦП и СКЗИ, которые реализуют ЭЦП и шифрование, достаточно для обеспечения подтверждения того, что электронный документ:

1) исходит от Участника Системы (подтверждение авторства документа);

2) не претерпел изменений при информационном взаимодействии Участников Системы в рамках Системы (подтверждение целостности и подлинности документа).

2. Участники Системы должны соблюдать установленный настоящим Регламентом порядок взаимодействия Участников Системы при обмене электронными документами и проверке их подлинности и достоверности. Система строится в соответствии с законодательством Кыргызской Республики. Все электронные документы, квитанции и протоколы, передаваемые в рамках Системы, должны быть заверены ЭЦП отправителя и переданы по специализированным (защищенным) каналам связи только в зашифрованном виде.

3. При обмене неформализованными сообщениями Участники Системы самостоятельно обеспечивают безопасность использования электронных документов средствами антивирусной защиты.

4. Датой исполнения налогоплательщиком обязательства по представлению налоговой отчетности в электронном виде посредством СЭО в соответствии с пунктом 2 статьи 89 Налогового Кодекса Кыргызской Республики является дата ее отправки, зафиксированная в подтверждении специализированного оператора сервиса об отправке электронного документа.

5. В случае нарушения правил использования СКЗИ и/или возникновения конфликтных ситуаций, связанных с подтверждением авторства и/или подлинности электронных документов, заверенных ЭЦП, а также в иных конфликтных ситуациях, связанных с представлением налоговой отчетности посредством СЭО, Стороны руководствуются порядком разрешения конфликтных ситуаций, изложенным в главе 4 настоящего Регламента.

Термины, используемые в настоящем Регламенте

6. В настоящем Регламенте используются следующие термины и определения:

1) **Закрытый (секретный) ключ ЭЦП** - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи и шифрования информации.

2) **Информационная система налоговых органов** - сервис органов налоговой службы по представлению налоговой отчетности в электронном виде.

3) **Информационный обмен** - обмен электронными документами между Участниками Системы в процессе их взаимодействия в рамках Системы.

4) **Сообщение о доставке** - электронный документ, удостоверяющий факт доставки налоговой отчетности в налоговый орган.

5) **Компрометация ключа ЭЦП** -7895123

6) утрата доверия к тому, что используемые закрытые ключи ЭЦП обеспечивают безопасность информации.

7) **Конфиденциальная информация** - требующая защиты информация, доступ к которой ограничивается в соответствии со статьей 54 Налогового кодекса Кыргызской Республики.

8) **Конфликтная ситуация** - ситуация, при которой у Участников Системы возникает необходимость разрешить вопросы, связанные с передачей и приемом электронных документов посредством СЭО, а также вопросы признания или непризнания авторства и/или подлинности электронных документов, обработанных средствами криптографической защиты информации.

9) **Кураторское приложение** - сервис, предназначенный для приема, проверки поступленияналоговой отчетности от налогоплательщиков для ответственных лиц налоговых органов.

10) **Налоговые органы** - территориальные управления Государственной налоговой службы при Правительстве Кыргызской Республики.

11) **Налоговая отчетность в электронном виде** - электронный документ в виде файла установленного формата, содержащий данные налоговой отчетности, утвержденной в установленном порядке в соответствии с Налоговым кодексом Кыргызской Республики.

12) **Некорректный электронный документ** - электронный документ, не прошедший процедуры проверки ЭЦП, имеющий искажения в тексте сообщения, не позволяющие понять его смысл или содержащий реквизиты отправителя, не соответствующие реквизитам, закрепленным за владельцем СКП, подписью которого заверен документ.

13) **Несанкционированный доступ** (НСД) **к информации** - доступ к информации, нарушающий установленные правила разграничения доступа.

14) **Неформализованное сообщение** - сообщение в виде электронного документа, для которого не существует утвержденного электронного формата представления.

15) **Открытый ключ ЭЦП** - уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная любому Участнику информационной системы и предназначенная для подтверждения с использованием средств ЭЦП подлинности электронной цифровой подписи в электронном документе. Открытый ключ Участника Системы является действующим на момент подписания, если он зарегистрирован (сертифицирован) и введен в действие.

16) **Подтверждение об отправке электронного документа** - электронный документ, содержащий время и дату отправки налоговой отчетности налогоплательщиком в соответствии с частью 2 статьи 89 Налогового кодекса Кыргызской Республики, и данные, идентифицирующие соответствующую налоговую отчетность.

17) **Протокол приема (протокол входного контроля)** - электронный документ, отражающий результаты приема отчета налоговым органом и содержащий информацию о факте приема отчета в информационную систему налоговых органов без замечаний либо требование об устранении нарушений с указанием допущенных нарушений согласно п.4 ст.89 Налогового кодекса Кыргызской Республики.

18) **Сертификат ключа подписи (далее - СКП)** - документ на бумажном носителе или электронный документ с ЭЦП уполномоченного должностного лица Удостоверяющего центра, включающий в себя открытый ключ ЭЦП и/или шифрования, которые выдаются Удостоверяющим центром участнику информационного обмена электронным документами для подтверждения подлинности ЭЦП, идентификации владельца сертификата ключа подписи и/или обеспечения защиты от искажения информации в электронном документе.

19) **Система информационного взаимодействия (далее - Система)** - совокупность методов и средств, используемых ее Участниками в процессе обмена электронными документами через СЭО при представлении налоговой отчетности в электронном виде.

20) **Системы электронной отчетности (далее - СЭО)** - совокупность программных и аппаратных средств, обеспечивающих представление налогоплательщиками налоговой отчетности в налоговые органы по общедоступным каналам связи и предоставление информационных услуг в электронном виде.

21) **Специализированный оператор** - предприятие, предоставляющее услуги по передаче электронных документов с применением ЭЦП между налогоплательщиками и налоговыми органами по специализированным (защищенным) каналам связи.

22) **Средства криптографической защиты информации (далее - СКЗИ)** - сертифицированные в порядке, установленном нормативно-правовыми актами Кыргызской Республики, аппаратные и/или программные средства, обеспечивающие шифрование, контроль целостности и применение ЭЦП при обмене электронными документами в Системе и совместимые с СКЗИ, используемыми в Системе.

23) **Уполномоченный налоговый орган** - Государственная налоговая служба при Правительстве Кыргызской Республики (далее – ГНС)

24) **Участники Системы** - ГНС, налоговые органы, налогоплательщики, представляющие налоговую отчетность в электронном виде через СЭО, и специализированный оператор сервиса услуг по передаче электронной отчетности.

25) **Формат представления электронных документов** - формализованное описание состава, структуры, а также требований к формированию представляемых в электронном виде показателей налоговой отчетности и документов, определенных ГНС для обеспечения информационного обслуживания налогоплательщиков.

26) **Шифрование** - способ преобразования открытой информации в закрытую информацию и обратно с целью обеспечения конфиденциальности информации.

27) **Электронный документ** - документ, представленный в электронном виде, в соответствии с требованиями формата для данного вида документа.

28) **Электронная цифровая подпись (ЭЦП)** - реквизит электронного документа, предназначенный для защиты данного электронного документа, от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

29) **ЭЦП налогоплательщика** - электронная цифровая подпись, владельцем сертификата ключа которой является должностное лицо налогоплательщика, использующее средства ЭЦП в рамках Системы.

30) **ЭЦП налогового органа** - электронная цифровая подпись, владельцем сертификата ключа которой является уполномоченное должностное лицо налогового органа, использующее средства ЭЦП в рамках Системы.

Глава 2. Порядок взаимодействия Участников Системы

7. Любая операция, выполняемая Участниками в рамках Системы, относится в целом к процессу обмена электронными документами между налоговыми органами и специализированным Оператором сервиса.

8. С целью защиты информации при информационном обмене должны применяться средства защиты информации (СКЗИ).

9. Электронный вид представляемых форм налоговой отчетности разрабатывается и сопровождается в соответствии с требуемыми ГНС формами. Формы представления налоговой отчетности в электронном виде и их описания доступны на веб-сайте Уполномоченного налогового органа.

10. Налогоплательщик в установленные сроки передает налоговую отчетность в утвержденном электронном формате посредством СЭО, заверив ее ЭЦП.

11. При получении налоговой отчетности от налогоплательщика специализированный Оператор сервиса:

1) проверяет подлинность ЭЦП налогоплательщика;

2) фиксирует время и дату получения налоговой отчетности от налогоплательщика;

3) формирует подтверждение об отправке электронного документа;

4) подписывает подтверждение об отправке электронного документа ЭЦП уполномоченного лица специализированного оператора сервиса;

5) отправляет налоговую отчетность и подтверждение специализированного оператора сервиса с соответствующими ЭЦП в адрес налогового органа в режиме «on-line»;

6) одновременно отправляет подтверждение об отправке электронного документа в адресналогоплательщика со статусом «Ожидает проверки».

12. Налоговый орган не позднее следующего рабочего дня с момента получения от специализированного оператора сервиса налоговой отчетности налогоплательщика и подтверждения об отправке электронного документа:

1) формирует сообщение о доставке налоговой отчетности;

2) подписывает сообщение о доставке налоговой отчетности ЭЦП уполномоченного лица налогового органа;

3) отправляет сообщение о доставке налоговой отчетности в адрес специализированного оператора сервиса для доставки налогоплательщику;

4) не позднее следующего рабочего дня загружает налоговую отчетность в информационную систему налогового органа, и формирует протокол входного контроля (протокол приема) налоговой отчетности. Протокол приема содержит сообщение о приеме налоговой отчетности без замечаний со статусом «Отчет принят» либо сообщение об отклонении отчета с указанием причин отклонения со статусом «Отчет не принят»;

5) подписывает протокол приема ЭЦП уполномоченного лица налогового органа;

6) шифрует протокол приема открытым ключом уполномоченного лица налоговогооргана;

7) отправляет протокол приема в адрес специализированного оператора сервиса длядоставки налогоплательщику.

13. Специализированный Оператор сервиса при получении от налогового органа квитанции о доставке и протокола приема направляет данные документы в адрес налогоплательщика.

14. В случае введения в действие новых форм налоговой отчетности и/или внесения в установленном порядке изменений в действующие формы налоговой отчетности ГНС размещает на сайте ГНС, утвержденные формы.

15. Специализированный Оператор сервиса в течение 10 рабочих дней после утверждения форм налоговой отчетности обязан внести соответствующие изменения в СЭО.

Действия Участников Системы в случае компрометации ключей ЭЦП

16. Специализированный оператор сервиса уведомляет Участников Системы о поступивших фактах, которые существенным образом могут сказаться на возможности дальнейшего использования СКЗИ и СКП.

17. Участник Системы в случае компрометации собственных ключей ЭЦП обязан немедленно по телефонным каналам связи с использованием устного пароля или факсимильным сообщением, заверенным подписью и печатью Участника информировать Специализированного оператора сервиса о наступлении события, трактуемого как компрометация.

18. При компрометации ключа ЭЦП Участник Системы обязан прекратить обмен электронными документами с другими Участниками Системы.

19. Специализированный оператор сервиса, получивший сообщение о компрометации ключей Участник Системы, должен убедиться в достоверности сообщения о компрометации (запросить пароль или факсимильное сообщение, заверенное подписью и печатью Участника Системы) и после этого обязан немедленно аннулировать скомпрометированные ключи ЭЦП (занести в Список отозванных сертификатов соответствующие СКП).

20. Участник Системы, объявивший о компрометации собственных криптографических ключей, в течение одного рабочего дня должен документально оформить уведомление и направить его Специализированному оператору сервиса.

21. Участник Системы, допустивший компрометацию собственных криптографических ключей, несет все издержки, связанные с генерацией новых ключей, их сертификацией и вводом в действие.

22. При возникновении внештатных ситуаций, таких, как выход из строя ключевого носителя, сбои и отказы в работе СКЗИ, сбои и отказы в работе средств ЭЦП и др., Участник Системы обязан:

1) сообщить о возникшей ситуации другим участникам системы;

2) выполнить указания специализированного Оператора связи, касающиеся выхода из данной внештатной ситуации.

Порядок разрешения конфликтных ситуаций, возникающих при информационном обмене в рамках Системы

23. При возникновении конфликтной ситуации, по содержанию электронного документа, для разрешения спора создается комиссия с привлечением всех сторон, организуется экспертиза, на основании которой выносится решение о корректности ЭЦП в данном электронном документе.

24. При возникновении конфликтной ситуации, по дате поступления электронного документа от отправителя получателю, решение о фактической дате поступления документа выносится на основании архивных файлов подтверждений отправки, подписанных ЭЦП налогового органа и налогоплательщика.

25. Разрешая конфликтные ситуации при нарушении процедур криптографической защиты информации и/или установлении авторства и/или подлинности электронных документов, заверенных ЭЦП, Участники Системы исходят из того, что:

1) в соответствии с Законом Кыргызской Республики «Об электронном документе и электронной цифровой подписи» и Налоговым кодексом Кыргызской Республики, документ в электронном виде, заверенный ЭЦП, является документом, имеющим юридическую силу, аналогично бумажному документу, снабженному подписью и печатью;

2) подтверждением даты представления электронного документа, является получение отправителем подтверждения отправки электронного документа;

3) используемая в соответствии с настоящим Регламентом система защиты информации, которая обеспечивается ЭЦП и шифрованием, достаточна для защиты информации от несанкционированного доступа, подтверждения целостности, подлинности и авторства электронных документов, а также для разрешения конфликтных ситуаций по ним.

Глава 3. Обязанности Участников Системы

26. ГНС обязан:

1) соблюдать положения настоящего Регламента;

2) организовать работу налоговых органов по приему налоговой отчетности вэлектронном виде;

3) обеспечить бесперебойное функционирование информационной системы ГНС поприему и обработке налоговой отчетности;

4) заблаговременно уведомлять специализированного Оператора сервиса о введении в действие новых форм налоговой отчетности и /или соответствующих изменениях в формах налоговой отчетности, предоставлять их описание и порядок их заполнения для своевременного исполнения специализированным Оператором сервиса обязательства по обеспечению соответствия отчетности в СЭО введенному в действие формату и требованиям Налогового кодекса Кыргызской Республики;

5) в случае не готовности информационной системы ГНС к принятию новых/измененных форм отчетов, ГНС обязуется, не позднее следующего рабочего дня, проверить, поступившие отчеты в кураторское приложение, и сформировать протокол входного контроля (протокол приема) налоговой отчетности. Протокол приема должен содержать сообщение о приеме налоговой отчетности без замечаний со статусом «Отчет принят» либо сообщение об отклонении отчета с указанием причин отклонения со статусом «Отчет не принят»;

6) извещать специализированного Оператора сервиса о технических неполадках и/или профилактических работах информационной системы, длящиеся более 24 часов для соответствующего оповещения налогоплательщика, если эти неполадки и/или работы могут помешать своевременному исполнению налогоплательщиком обязательства по представлению налоговой отчетности в электронном виде;

7) своевременно извещать специализированного Оператора сервиса о каких-либо изменениях в работе информационной системы по приему и обработке налоговой отчетности для обеспечения совместимости СЭО с информационной системой ГНС.

8) незамедлительно приостановить обмен с Участниками Системы электронными документами, подписанными ЭЦП, при получении официального сообщения о компрометации этого ключа ЭЦП от специализированного Оператора сервиса;

27. Налоговый орган обязан:

1) соблюдать положения настоящего Регламента;

2) обеспечить своевременность представления в адрес специализированного Оператора сервиса сообщения о доставке и протокола приема налоговой отчетности для доставки их налогоплательщику;

28. Специализированный Оператор сервиса обязан:

1) соблюдать положения настоящего Регламента;

2) обеспечить правильный математическо-логический контроль вводимых данных налогоплательщиком;

3) фиксировать дату и время отправки налоговой отчетности налогоплательщиками и формировать соответствующие подтверждения;

4) в течение 10 рабочих дней после утверждения форм налоговой отчетности внести соответствующие изменения в СЭО;

5) обеспечить своевременность доставки налоговой отчетности и подтверждения об отправке электронного документа в адрес налогового органа, протокола приема и сообщения о доставке в адрес налогоплательщика в соответствии с требованиями нормативно-правовых актов и налогового законодательства, касающихся работы СЭО;

6) начиная со дня ввода в действие формата электронного представления форм налоговой отчетности, обеспечить соответствие отчетности в СЭО введенному в действие формату и требованиям Налогового кодекса Кыргызской Республики;

7) в случае временного отсутствия доступа к информационной системе ГНС сохранить электронные документы, переданные налогоплательщиком в налоговые органы посредством СЭО, на своем сервере и при возобновлении связи передать их на сервер ГНС;

8) в процессе обеспечения информационного обмена в рамках Системы осуществлять регулирование отношений с Участниками Системы в соответствии с Законом Кыргызской Республики «Об электронном документе и электронной цифровой подписи», Законом Кыргызской Республики «Об информации персонального характера», а также настоящим Регламентом;

9) предоставлять по согласованной форме ежемесячно к 25 числу информацию в ГНС, а также предоставлять информацию по запросам ГНС.

29. Специализированный оператор сервиса имеет право на:

1) своевременное извещение налоговым органом о технических неполадках и/или профилактических работах информационной системы налогового органа для соответствующего оповещения налогоплательщика, если эти неполадки и/или работы могут помешать своевременному исполнению налогоплательщиком обязательства по представлению налоговой отчетности в электронном виде;

2) своевременное извещение налоговым органом о каких-либо изменениях в работе его информационной системы по приему и обработке налоговой отчетности для обеспечения совместимости СЭО с информационной системой ГНС;

3) получение квалифицированной консультации налоговых органов по вопросу функционирования информационной системы ГНС, а также методологической помощи по вопросу заполнения форм налоговой отчетности.

30. Участники Системы обязаны хранить в тайне закрытые ключи ЭЦП и принимать мерыдля предотвращения их компрометации.

31. Участник Системы имеет право запрашивать подтверждения по полученным электронным документам в случае возникновения сомнений в их подлинности, требовать исполнения обязательств по принятым электронным документам от других Участников Системы.

32. Участникам Системы запрещается принимать к исполнению электронные документы с ЭЦП в следующих случаях:

1) сертификат ключа подписи отправителя утратил силу на момент создания ЭЦП в документе;

2) не подтверждена подлинность ЭЦП в электронном документе;

3) использование ЭЦП не соответствует сведениям, указанным в СКП;

4) электронный документ с ЭЦП лица, не имеющего права на утверждение данного документа.

Глава 4. Ответственность Участников Системы (ГНС и специализированный оператор)

33. Участники Системы несут ответственность за правильность исполнения обязательств и соблюдение условий настоящего Регламента.

34. В случаях неисполнения или ненадлежащего исполнения обязательств, принятых на себя Участниками по условиям настоящего Регламента, Участники несут ответственность в соответствии с положениями настоящего Регламента, а в случаях, не предусмотренных настоящим Регламента – в соответствии с действующим законодательством Кыргызской Республики.

35. При аварийном отключении электроэнергии и иных обстоятельствах, повлекших за собой неспособность информационных систем обмениваться электронными документами, Участники должны незамедлительно известить друг друга в письменной форме.

36. В случае возникновения обстоятельств непреодолимой силы, препятствующих осуществлению Участниками своих обязательств по настоящему Соглашению, и иных обстоятельств, не зависящих от воли Участников, Участники освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых на себя обязательств на все время действия указанных обстоятельств. Участник, который не может выполнить свои обязательства по настоящему Соглашению по причине действия непреодолимой силы, должен в течение одного дня уведомить другого Участника Системы.

37. Под обстоятельствами непреодолимой силы Участники понимают обстоятельства, которые возникли после подписания настоящего Соглашения в результате возникновения чрезвычайных и неотвратимых обстоятельств в результате стихийных бедствий, таких как землетрясения, наводнения или иных обстоятельств, которые невозможно предусмотреть или предотвратить, либо возможно предусмотреть, но невозможно предотвратить.

38. Участник, ссылающийся на обстоятельства непреодолимой силы, обязан незамедлительно (не позднее, чем в 1-дневный срок с момента его наступления) известить другую сторону о наступлении этих обстоятельств. Извещение должно содержать данные о характере обстоятельств и оценку их влияния на возможность исполнения Участником своих обязательств. Несвоевременное извещение Участником о наступлении обстоятельств, освобождающих ее от ответственности, влечет за собой утрату права для этого Участника ссылаться на эти обстоятельства.

39. Вся информация полученная Участниками Системы в процессе взаимодействия в соответствии с действующим законодательством Кыргызской Республики, не подлежит разглашению Участниками или передаче третьим лицам ни при каких обстоятельствах, кроме случаев, предусмотренных законодательством Кыргызской Республики.

40. Налоговый орган несет ответственность перед налогоплательщиком за своевременность обработки информации, поступающей от налогоплательщиков в электронном виде, с применением ЭЦП, по специализированным (защищенным) каналам связи и предоставление всех необходимых подтверждений и сообщений о доставке в электронном виде.

41. ГНС несет ответственность за своевременное доведение до сведений Участников Системы информации об изменении в представлении налоговой отчетности в электронном виде по общедоступным каналам связи, публикуя соответствующую информацию на открытом информационном вебсайте ГНС и уведомлением специализированного Оператора сервиса.

42. Специализированный Оператор сервиса не несет ответственность за содержание налоговой отчетности, передаваемой налогоплательщиком посредством СЭО.

43. Специализированный Оператор сервиса не несёт ответственности перед владельцами СКП и лицами, использующими СКП для проверки подписи и шифрования, а также перед третьими лицами за любые убытки, потери, иной ущерб, связанный с использованием СКП, независимо от суммы, заключенных с использованием СКП сделок и совершения ими иных действий, за исключением случаев нарушения специализированным Оператором сервиса обязательств, предусмотренных настоящим Регламентом и действующим законодательством Кыргызской Республики.

Глава 5. Технические требования к используемым программным средствам

44. Применяемое средство криптографической защиты информации (средство электронной цифровой подписи) должно обеспечивать применение ЭЦП и шифрования в соответствии с нормами действующего законодательства Кыргызской Республики и поддерживать следующие объектные идентификаторы алгоритмов:

1) ГОСТ Р 34.10-94 1.2.643.2.2.20 «Алгоритм формирования открытых ключей»;
2) ГОСТ Р 34.10-2001 1.2.643.2.2.19 «Алгоритм формирования открытых ключей»;
3) ГОСТ Р 34.10-94 1.2.643.2.2.4 «Алгоритм подписи»;
4) Диффи-Хеллмана 1.2.643.2.2.99 «Алгоритм на базе экспоненциальной функции»;
5) Диффи-Хеллмана 1.2.643.2.2.98 «Алгоритм на базе эллиптической кривой»;
6) ГОСТ Р 34.11-94 1.2.643.2.2.9 «Алгоритм функции хеширования»;
7) ГОСТ 28147-89 1.2.643.2.2.21 «Алгоритм шифрования».

45. Применяемое средство криптографической защиты информации (средство электронной цифровой подписи) должно поддерживать сертификаты открытых ключей стандарта X.509v3 согласно RFC 5280 «Internet X.509 PublicKeyInfrastructure. Certificate and Certificate Revocation List (CRL) Profile» сучетом RFC 4491 «Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile».

46. Обязательными атрибутами поля идентификационных данных владельца сертификата, являющегося физическим лицом, и/или доверенного лица, представляющего юридическое лицо, являются:

1) CommonName (CN) (Общее Имя) - Фамилия, имя, отчество физического лица или доверенного лица, представляющего юридическое лицо;
2) SerialNumber - ИНН юридического лица или физического лица;
3) Organization (O) (Организация) - Наименование организации;
4) Location (L) (Локализация) - Место регистрации юридического лица или физического лица;
5) Country (C) - Страна.

47. Передача данных. Применяемое средство криптографической защиты информации (средство электронной цифровой подписи) обеспечивает криптографическое шифрование канала передачи данных по ГОСТ 28147-89 1.2.643.2.2.21 (VipNETClient)

48. Формат передачи данных представляет собой набор текстовых данных, который состоит из двух частей:

1) Данные отчета в формате XML (vl.O UTF-8) преобразованные в формат BASE-64, представленные в бинарном виде;

2) Сигнатура подписи отчета, удостоверяющая принадлежность отчета конкретному пользователю СЭО, преобразованная в формат BASE-64, представленная в бинарном виде.

49. Авторизация. Аутентификация пользователя в СЭО состоит из нескольких этапов:

1) Проверка ПИН-кода для доступа к контейнеру закрытого ключа подписи ЭЦП пользователя;

2) Проверка целостности ключа подписи ЭЦП;

3) Верификация ключа ЭЦП — проверка валидности ЭЦП;

4) Проверка регистрационных данных, полученных из контейнера закрытого ключа ЭЦП, с данными СЭО (на случай компрометации ЭЦП).

50. Средство криптографической защиты информации (средство электронной цифровой подписи) должно обеспечивать выполнение следующих сервисных функций:

1) установка личных сертификатов открытых ключей на рабочем месте/сервере с обеспечением связи сертификата открытого ключа с соответствующим указанному сертификату закрытым ключом;

2) копирование и удаление закрытых ключей;

3) установка, изменение и удаление пароля на доступ к закрытому ключу.

4) функционирование в среде операционных систем Windows XP/2003/Vista/7/2008/8.1/10.

51. Средство криптографической защиты информации (средство электронной цифровой подписи) должно поддерживать следующие носители:

1) Отчуждаемые носители eToken, RuToken;

2) Отчуждаемый носитель USB Flash, оптические носители;

3) Файловая система ПК;

4) СМАРТ-карты.