П Р И К А З

МИНИСТРА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

№ 404

6 июля 2016 г. г. Москва

Об утверждении Регламента Удостоверяющего центра Министерства обороны Российской Федерации

В соответствии с частью 7 статьи 13 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» **П Р И К А З Ы В А Ю**:

1. Утвердить прилагаемый Регламент Удостоверяющего центра Министерства обороны Российской Федерации.

2. Предоставить Восьмому управлению Генерального штаба Вооруженных Сил Российской Федерации право давать органам военного управления, воинским частям и организациям Вооруженных Сил Российской Федерации разъяснения по вопросам применения Регламента Удостоверяющего центра Министерства обороны Российской Федерации и функционирования Удостоверяющего центра Министерства обороны Российской Федерации.

3. Признать утратившим силу Регламент Удостоверяющего центра Министерства обороны Российской Федерации при обработке информации, не содержащей сведения, составляющие государственную тайну, утвержденный заместителем Министра обороны Российской Федерации 2 октября 2012 г.

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ МИНИСТРА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
генерал армии

В.Герасимов

Приложение
к приказу Министра обороны
Российской Федерации
от 6 июля 2016 г. № 404

РЕГЛАМЕНТ
Удостоверяющего центра Министерства обороны Российской Федерации

I. Общие положения

1. Настоящий Регламент Удостоверяющего центра Министерства обороны Российской Федерации (далее – Регламент) разработан в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон) и нормативными правовыми актами Российской Федерации, регулирующими деятельность удостоверяющих центров.

2. Восьмое управление Генерального штаба Вооруженных Сил Российской Федерации[*] осуществляет организацию функционирования Удостоверяющего центра[**].

3. Настоящий Регламент определяет порядок реализации функций Удостоверяющего центра, осуществления его прав и исполнения обязанностей.

4. Размещение настоящего Регламента, а также сертификата ключа проверки электронной подписи Удостоверяющего центра осуществляется на официальном сайте Министерства обороны в информационно-телекоммуникационной сети «Интернет» и в автоматизированной информационной системе электронного документооборота Министерства обороны.

5. Контактные телефоны Удостоверяющего центра: (495)696-27-75, (495)696-27-23, (495)696-94-86.

---

[*] Далее в тексте настоящего Регламента, если не оговорено особо, для краткости будут именоваться: Восьмое управление Генерального штаба Вооруженных Сил Российской Федерации – Восьмым управлением; Министерство обороны Российской Федерации – Министерством обороны; Вооруженные Силы Российской Федерации – Вооруженными Силами; Министр обороны Российской Федерации и его заместители – руководящими должностными лицами Министерства обороны; органы военного управления, объединения, соединения, воинские части и организации Вооруженных Сил Российской Федерации – организациями; Удостоверяющий центр Министерства обороны Российской Федерации, аккредитованный федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, – Удостоверяющим центром.

[**] В соответствии с Положением о Восьмом управлении Генерального штаба Вооруженных Сил Российской Федерации, утвержденным приказом Министра обороны Российской Федерации от 28 декабря 2013 г. № 0113.

Подробная контактная и справочная информация об Удостоверяющем центре размещается на официальном сайте Министерства обороны в информационно-телекоммуникационной сети «Интернет».

6. В настоящем Регламенте используются следующие основные понятия:

электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи;

ключевой носитель – отчуждаемый машинный носитель, содержащий ключ электронной подписи;

компрометация ключа электронной подписи – хищение, утрата (в том числе с последующим обнаружением), разглашение, несанкционированный доступ и другие происшествия с ключом электронной подписи или его носителем, повлекшие нарушение конфиденциальности ключа электронной подписи;

ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи;

средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданный удостоверяющими центрами либо доверенными лицами удостоверяющих центров и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

квалифицированный сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат) – сертификат ключа проверки электронной подписи, созданный Удостоверяющим центром и соответствующий требованиям, установленным Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами;

владелец квалифицированного сертификата ключа проверки электронной подписи (далее – владелец квалифицированного сертификата) – лицо, которому в установленном порядке выдан квалифицированный сертификат;

реестр квалифицированных сертификатов – реестр выданных и аннулированных Удостоверяющим центром квалифицированных сертификатов, в том числе включающий в себя информацию, содержащуюся в выданных Удостоверяющим центром квалифицированных сертификатах, информацию о датах прекращения действия или аннулирования квалифицированных сертификатов и об основаниях таких прекращения или аннулирования;

список аннулированных сертификатов – электронный документ, подписанный электронной подписью Удостоверяющего центра, представляющий собой список уникальных серийных номеров сертификатов ключей проверки электронных подписей, которые были аннулированы или действие которых было приостановлено (прекращено);

участники электронного (информационного) взаимодействия – организации и их должностные лица, осуществляющие обмен информацией в электронной форме в государственных информационных системах или информационных (автоматизированных) системах Министерства обороны с использованием созданных в Удостоверяющем центре ключей электронных подписей и квалифицированных сертификатов;

заявители – участники электронного (информационного) взаимодействия, обратившиеся за получением ключей электронных подписей и квалифицированных сертификатов в порядке, установленном настоящим Регламентом;

доверенное лицо – представитель заявителя, действующий от его имени на основании доверенности, уполномоченный на получение в Удостоверяющем центре ключевого носителя и комплекта документов, необходимых для использования средств электронной подписи;

ответственное должностное лицо – должностное лицо, уполномоченное руководящим должностным лицом Министерства обороны – владельцем квалифицированного сертификата на получение и хранение ключевого носителя и использование ключа электронной подписи;

доверенное лицо Удостоверяющего центра – должностное лицо, наделенное полномочиями по передаче изготовленного Удостоверяющим центром квалифицированного сертификата его владельцу в соответствии с требованиями настоящего Регламента.

7. Срок действия ключа электронной подписи, используемого средствами Удостоверяющего центра, должен соответствовать требованиям, установленным к средствам электронной подписи[*].

8. Удостоверяющий центр:

создает по заявкам, а также в соответствии с решениями руководящих должностных лиц Министерства обороны ключи электронных подписей и квалифицированные сертификаты;

---

[*] Пункт 27.2 Требований к средствам удостоверяющего центра, утвержденных приказом Федеральной службы безопасности Российской Федерации от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

выдает квалифицированные сертификаты в форме документов на бумажных носителях и (или) в форме электронных документов;

устанавливает сроки действия квалифицированных сертификатов;

аннулирует (прекращает действие), приостанавливает и возобновляет действие квалифицированных сертификатов;

ведет реестр квалифицированных сертификатов, обеспечивает его актуальность;

предоставляет в электронной форме копии квалифицированных сертификатов их владельцам;

устанавливает порядок и обеспечивает доступ участников электронного (информационного) взаимодействия к информации, содержащейся в реестре квалифицированных сертификатов, в том числе с использованием информационно-телекоммуникационной сети «Интернет»;

проверяет уникальность ключей проверки электронных подписей в реестре квалифицированных сертификатов;

осуществляет по обращениям участников электронного (информационного) взаимодействия проверку подлинности электронных подписей;

осуществляет иную деятельность, связанную с использованием электронной подписи.

9. Удостоверяющий центр обязан:

информировать в письменной форме заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

обеспечивать актуальность информации, содержащейся в реестре квалифицированных сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком информацию, содержащуюся в реестре квалифицированных сертификатов, в том числе информацию об аннулировании квалифицированного сертификата;

обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей;

отказать заявителю в создании квалифицированного сертификата в случае, если не было подтверждено, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения квалифицированного сертификата;

отказать заявителю в создании квалифицированного сертификата в случае отрицательного результата проверки в реестре квалифицированных сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения квалифицированного сертификата.

10. При вручении квалифицированного сертификата доверенное лицо Удостоверяющего центра устанавливает личность заявителя либо полномо-

чия его доверенного лица по обращению за получением данного сертификата и обеспечивает передачу ему необходимого комплекта документов в соответствии с требованиями настоящего Регламента.

11. Удостоверяющий центр информирует участников электронного (информационного) взаимодействия о необходимости:

обеспечивать конфиденциальность ключей электронных подписей, в частности, не допускать использования ключей электронных подписей без согласия их владельцев;

своевременно уведомлять Удостоверяющий центр и иных участников электронного (информационного) взаимодействия о нарушении конфиденциальности ключей электронных подписей (не более одного рабочего дня со дня получения информации о таком нарушении);

не допускать использования ключей электронных подписей при наличии оснований полагать, что их конфиденциальность нарушена;

использовать ключи электронных подписей с учетом ограничений, содержащихся в квалифицированных сертификатах;

использовать для создания и проверки электронных подписей средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным Федеральным законом.

II. Порядок создания и выдачи ключей электронных подписей и квалифицированных сертификатов

12. Создание ключей электронных подписей и квалифицированных сертификатов должностным лицам организаций осуществляется Удостоверяющим центром на основании заявки на создание ключей электронных подписей и сертификатов ключей проверки электронных подписей по форме согласно приложению № 1 к настоящему Регламенту.

13. Создание ключей электронных подписей и квалифицированных сертификатов организациям, являющимся юридическими лицами (далее – юридические лица), осуществляется Удостоверяющим центром на основании заявки на создание ключей электронных подписей и сертификатов ключей проверки электронных подписей юридического лица по форме согласно приложению № 2 к настоящему Регламенту, в которой указываются лица, действующие от имени юридического лица на основании учредительных документов юридического лица или доверенности (далее – уполномоченные лица).

Создание ключей электронных подписей и квалифицированных сертификатов юридическим лицам, используемых для автоматического создания и (или) автоматической проверки электронных подписей, осуществляется Удостоверяющим центром на основании заявки на создание ключей электронных подписей и сертификатов ключей проверки электронных подписей юридического лица для автоматического создания электронных подписей по форме согласно приложению № 3 к настоящему Регламенту.

Вместе с заявками, указанными в настоящем пункте, в Удостоверяющий центр представляются документы или их надлежащим образом заверенные копии для подтверждения содержащихся в них сведений о юридическом лице:

документ, подтверждающий факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц, – для подтверждения основного государственного регистрационного номера (ОГРН);

свидетельство о постановке на учет в налоговом органе – для подтверждения идентификационного номера налогоплательщика (ИНН).

14. Удостоверяющий центр проверяет соответствие сведений, содержащихся в соответствующей заявке на создание ключей электронных подписей и сертификатов ключей проверки электронных подписей, а также прилагаемых к ней документов требованиям настоящего Регламента.

По результатам проверки Удостоверяющий центр направляет заявителю уведомление об изготовлении (отказе в изготовлении) квалифицированных сертификатов. В уведомлении об отказе в изготовлении квалифицированных сертификатов указывается причина отклонения заявки.

Уведомление об изготовлении (отказе в изготовлении) квалифицированных сертификатов направляется в письменном виде и в электронном виде – на адрес электронной почты, указанный в заявке.

15. При принятии положительного решения об изготовлении квалифицированных сертификатов в срок до 5 рабочих дней с момента получения Удостоверяющим центром соответствующей заявки на создание ключей электронных подписей и сертификатов ключей проверки электронных подписей Удостоверяющий центр осуществляет:

создание и запись ключа электронной подписи и квалифицированного сертификата на ключевой носитель;

изготовление квалифицированного сертификата на бумажном носителе в двух экземплярах.

16. Для получения квалифицированных сертификатов заявитель или доверенное лицо прибывает в Удостоверяющий центр.

17. После установления личности заявителя (доверенного лица), а в соответствующих случаях после подтверждения полномочий лица действовать от имени юридического лица и полномочий доверенного лица на получение квалифицированных сертификатов Удостоверяющий центр выдает заявителю (доверенному лицу):

ключевой носитель с ключом электронной подписи и квалифицированным сертификатом;

два экземпляра квалифицированного сертификата на бумажном носителе, подписанные должностным лицом Удостоверяющего центра (доверенным лицом Удостоверяющего центра);

ключевую фразу и парольное значение доступа к ключевому носителю в запечатанном виде;

руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи (при первичной выдаче квалифицированного сертификата).

После ознакомления заявителя с информацией, содержащейся в квалифицированном сертификате на бумажном носителе (под подпись на каждом экземпляре), один экземпляр квалифицированного сертификата возвращается в Удостоверяющий центр не позднее 3 дней с даты его получения.

III. Особенности создания и выдачи квалифицированных сертификатов руководящих должностных лиц Министерства обороны

18. Создание квалифицированных сертификатов руководящих должностных лиц Министерства обороны осуществляется на основании их письменных решений (согласий) (далее – решение о создании квалифицированного сертификата).

Решение о создании квалифицированного сертификата должно включать согласие руководящего должностного лица Министерства обороны на получение и обработку Удостоверяющим центром его персональных данных в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»).

19. Для принятия решения о создании квалифицированного сертификата на имя руководящего должностного лица Министерства обороны заинтересованным органом военного управления в установленном порядке подготавливается доклад, в который включаются:

предназначение квалифицированного сертификата;

согласие на передачу персональных данных руководящего должностного лица Министерства обороны (фамилия, имя, отчество, ИНН, страховой номер индивидуального лицевого счета (СНИЛС), серия и номер основного документа, удостоверяющего личность) в Удостоверяющий центр для их обработки в соответствии с требованиями Федерального закона «О персональных данных»;

предложение о назначении ответственного должностного лица с указанием его фамилии, имени, отчества, серии и номера основного документа, удостоверяющего личность.

Проект доклада до представления руководящему должностному лицу Министерства обороны подлежит согласованию с Восьмым управлением и другими заинтересованными органами военного управления.

20. Решение о создании квалифицированного сертификата доводится в установленном порядке до Удостоверяющего центра (через Восьмое управление) и других заинтересованных органов военного управления.

21. На основании решения о создании квалифицированного сертификата Удостоверяющий центр создает квалифицированный сертификат и уведомляет ответственное должностное лицо.

22. Для получения квалифицированного сертификата ответственное должностное лицо прибывает в Удостоверяющий центр.

23. После установления личности ответственного должностного лица и подтверждения его полномочий на получение квалифицированного сертификата Удостоверяющий центр выдает ответственному должностному лицу:

ключевой носитель с ключом электронной подписи и квалифицированным сертификатом;

квалифицированный сертификат на бумажном носителе, подписанный должностным лицом Удостоверяющего центра (доверенным лицом Удостоверяющего центра);

ключевую фразу и парольное значение доступа к ключевому носителю в запечатанном виде;

руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи (при первичной выдаче квалифицированного сертификата).

Об ознакомлении с информацией, содержащейся в квалифицированном сертификате, ответственное должностное лицо расписывается на каждом экземпляре квалифицированного сертификата на бумажном носителе, один экземпляр которого остается в Удостоверяющем центре.

24. При переназначении или увольнении руководящего должностного лица Министерства обороны ответственное должностное лицо сдает ключевой носитель руководящего должностного лица Министерства обороны в Удостоверяющий центр для последующего уничтожения ключа электронной подписи.

25. Уничтожение ключа электронной подписи проводится комиссией Удостоверяющего центра в присутствии ответственного должностного лица с составлением акта об уничтожении.

26. О получении (уничтожении) квалифицированного сертификата ответственное должностное лицо при необходимости докладывает руководящему должностному лицу Министерства обороны – владельцу квалифицированного сертификата.

27. При переводе или увольнении ответственного должностного лица заинтересованным органом военного управления в установленном порядке подготавливается доклад на имя руководящего должностного лица Министерства обороны с учетом требований, изложенных в пункте 19 настоящего Регламента, содержащий предложения о назначении нового ответственного должностного лица.

IV. Плановая и внеплановая смена ключей электронных подписей и квалифицированных сертификатов

28. Удостоверяющий центр выполняет плановую смену ключей электронных подписей и изготовление новых квалифицированных сертификатов на основании заявок, направляемых в Удостоверяющий центр не ранее одного месяца и не позднее 15 календарных дней до окончания срока действия ключа электронной подписи.

29. Внеплановая смена ключей электронных подписей и квалифицированных сертификатов осуществляется Удостоверяющим центром в следующих случаях:

если участник электронного (информационного) взаимодействия в установленные сроки не осуществил плановую смену ключа электронной подписи и квалифицированного сертификата;

компрометации ключа электронной подписи;

изменения данных участника электронного (информационного) взаимодействия, указанных в квалифицированном сертификате.

30. Плановая и внеплановая смена ключей электронных подписей и квалифицированных сертификатов осуществляется в порядке, изложенном в разделах II и III настоящего Регламента.

V. Аннулирование (прекращение действия) и изменение статуса квалифицированных сертификатов

31. Удостоверяющий центр аннулирует (прекращает действие) квалифицированные сертификаты в случаях:

истечения установленных сроков их действия;

истечения сроков, на которые действие квалифицированных сертификатов было приостановлено, если в установленные сроки в Удостоверяющий центр не были представлены заявки на возобновление их действия;

получения от участника электронного (информационного) взаимодействия заявки на аннулирование (прекращение действия) сертификатов ключей проверки электронных подписей по форме согласно приложению № 4 к настоящему Регламенту;

компрометации ключей электронных подписей;

неподтверждения, что владелец квалифицированного сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в квалифицированном сертификате;

установления, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи содержится в ином, ранее созданном квалифицированном сертификате;

вступления в силу решения суда, которым установлено, что квалифицированный сертификат содержит недостоверную информацию;

прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам.

32. Удостоверяющий центр аннулирует (прекращает действие) квалифицированный сертификат в течение 12 часов с момента получения заявки на аннулирование (прекращение действия) сертификатов ключей проверки электронных подписей при соответствии указанных в ней сведений данным реестра квалифицированных сертификатов. Действие квалифицированного сертификата прекращается с момента внесения записи об этом в реестр квалифицированных сертификатов.

В случае выявления несоответствия сведений, содержащихся в заявке на аннулирование (прекращение действия) сертификатов ключей проверки электронных подписей и данных реестра квалифицированных сертификатов, указанная заявка отклоняется, а участник электронного (информационного) взаимодействия уведомляется с указанием причины отказа в аннулировании (прекращении действия) квалифицированного сертификата.

33. До внесения в реестр квалифицированных сертификатов информации об аннулировании квалифицированного сертификата Удостоверяющий центр обязан уведомить владельца квалифицированного сертификата путем направления документа на бумажном носителе или электронного документа.

34. Опубликование первого (наиболее раннего) списка аннулированных сертификатов, содержащего сведения о квалифицированном сертификате, который был аннулирован (действие которого было прекращено), и изданного не ранее времени наступления события, повлекшего аннулирование (прекращение действия) квалифицированного сертификата, является уведомлением участников электронного (информационного) взаимодействия о факте аннулирования (прекращения действия) квалифицированного сертификата.

35. Удостоверяющий центр приостанавливает действие квалифицированных сертификатов в следующих случаях:

получения от участника электронного (информационного) взаимодействия заявки на изменение статуса сертификатов ключей проверки электронных подписей по форме согласно приложению № 5 к настоящему Регламенту;

по заявлению владельца квалифицированного сертификата в устной форме, в том числе по телефону;

по решению Удостоверяющего центра в случаях, предусмотренных настоящим Регламентом.

36. Действие квалифицированных сертификатов приостанавливается на исчисляемый в календарных днях срок. Минимальный срок приостановле-

ния действия квалифицированных сертификатов составляет 15 календарных дней, максимальный – 30 календарных дней.

37. Если в течение срока приостановления действия квалифицированного сертификата действие этого сертификата не будет возобновлено, Удостоверяющий центр прекращает действие указанного квалифицированного сертификата.

38. Удостоверяющий центр приостанавливает или возобновляет действие квалифицированных сертификатов в течение 12 часов с момента получения названной заявки при соответствии указанных в ней сведений данным реестра квалифицированных сертификатов. Действие квалифицированного сертификата приостанавливается (возобновляется) с момента внесения записи об этом в реестр квалифицированных сертификатов.

В случае выявления несоответствия сведений, содержащихся в заявке на изменение статуса сертификатов ключей проверки электронных подписей и данных реестра квалифицированных сертификатов, указанная заявка отклоняется, а участник электронного (информационного) взаимодействия уведомляется с указанием причины отказа в изменении статуса квалифицированного сертификата.

39. Опубликование первого (наиболее раннего) списка аннулированных сертификатов, содержащего сведения о квалифицированном сертификате, действие которого было приостановлено, и изданного не ранее времени наступления события, повлекшего приостановление действия квалифицированного сертификата, является уведомлением участников электронного (информационного) взаимодействия о факте приостановления действия квалифицированного сертификата.

40. Информация о размещении списка аннулированных сертификатов указывается Удостоверяющим центром в квалифицированном сертификате в расширении «Точки распространения списков аннулированных сертификатов (CRL Distribution Points)».

При внесении изменений в список аннулированных сертификатов его размещение осуществляется Удостоверяющим центром в течение 12 часов.

Периодичность обновления списка аннулированных сертификатов устанавливается Удостоверяющим центром.

41. Приостановление действия квалифицированных сертификатов по заявлению владельцев квалифицированных сертификатов в устной форме осуществляется при подозрении в компрометации ключей электронных подписей или при возникновении обстоятельств, требующих оперативного приостановления действия квалифицированных сертификатов.

42. В заявлении в устной форме владелец квалифицированного сертификата сообщает должностному лицу Удостоверяющего центра следующую информацию:

идентификационные данные владельца квалифицированного сертификата, действие которого необходимо приостановить;

серийный номер квалифицированного сертификата, действие которого необходимо приостановить;

причина, по которой действие квалифицированного сертификата приостанавливается;

срок, на который приостанавливается действие квалифицированного сертификата;

ключевую фразу.

43. Заявление владельца квалифицированного сертификата в устной форме принимается должностным лицом Удостоверяющего центра только в случае положительной аутентификации владельца квалифицированного сертификата (совпадения ключевой фразы, сообщенной заявителем, с данными реестра квалифицированных сертификатов).

Удостоверяющий центр приостанавливает действие квалифицированного сертификата в возможно короткий срок, но не позднее 12 часов с момента получения указанного заявления.

44. Решение о компрометации (подозрении в компрометации) ключа электронной подписи принимается владельцем квалифицированного сертификата самостоятельно.

45. Удостоверяющий центр вправе аннулировать (прекратить действие) или приостановить действие квалифицированного сертификата при компрометации или подозрении в компрометации ключа электронной подписи (в том числе, если владельцу квалифицированного сертификата не было известно о возможном факте компрометации ключа).

В этом случае Удостоверяющий центр сообщает владельцу квалифицированного сертификата о наступлении события, повлекшего прекращение действия или приостановление действия квалифицированного сертификата.

VI. Получение информации о статусе квалифицированных сертификатов

46. Для получения информации о статусе квалифицированных сертификатов в Удостоверяющий центр направляется заявка на получение информации о статусе сертификатов ключей проверки электронных подписей по форме согласно приложению № 6 к настоящему Регламенту.

47. По результатам рассмотрения и обработки заявки на получение информации о статусе сертификатов ключей проверки электронных подписей Удостоверяющим центром оформляется справка о статусе квалифицированного сертификата, которая направляется участнику электронного (информационного) взаимодействия или владельцу квалифицированного сертификата.

48. Предоставление справки о статусе квалифицированного сертификата осуществляется Удостоверяющим центром в срок до 10 рабочих дней с момента получения соответствующей заявки.

VII. Действия при компрометации и подозрении в компрометации ключей электронных подписей

49. При компрометации ключа электронной подписи, а равно при подозрении на компрометацию участник электронного (информационного) взаимодействия или владелец квалифицированного сертификата незамедлительно прекращает работу с ключом электронной подписи и информирует Удостоверяющий центр в устной форме, в том числе по телефону, в порядке, изложенном в разделе V настоящего Регламента.

50. Информация о факте компрометации (подозрении в компрометации) ключа электронной подписи размещается Удостоверяющим центром на официальном сайте Министерства обороны в информационно-телекоммуникационной сети «Интернет».

51. При компрометации ключа электронной подписи Удостоверяющего центра прекращается действие всех подписанных им квалифицированных сертификатов.

Участники электронного (информационного) взаимодействия или владельцы квалифицированных сертификатов уведомляются о факте компрометации ключа Удостоверяющего центра путем размещения информации о данном факте на официальном сайте Министерства обороны в информационно-телекоммуникационной сети «Интернет».

52. Все действовавшие на момент компрометации ключа электронной подписи Удостоверяющего центра квалифицированные сертификаты, а также квалифицированные сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

Приложение № 1
к Регламенту (п. 12)

Форма

Начальнику 8 Управления
Генерального штаба Вооруженных Сил
Российской Федерации

ЗАЯВКА
на создание ключей электронных подписей и сертификатов ключей проверки электронных подписей
для применения __________
(указывается предназначение электронной подписи или наименование информационной системы, в которой планируется ее применение)

Прошу Ваших указаний о формировании ключей электронных подписей и изготовлении сертификатов ключей проверки электронных подписей следующему личному составу:

№ п/п	Фамилия, имя, отчество	Должность	Серия и номер паспорта	Наименование организации	Наименование подразделения (при наличии)	Страховой номер индивидуального лицевого счета (СНИЛС)	Идентификационный номер налогоплательщика (ИНН)	Адрес (край, область, город)	Адрес электронной почты, E-mail
1	2	3	4	5	6	7	8	9	10

Начальник (руководитель) _____
(наименование организации)

_____
(воинское звание, подпись, инициал имени, фамилия)

М.П.
«___» _____ 20__ г.

Примечания: 1. Подпись начальника (руководителя) заверяется печатью установленного образца.

2. В заявке дополнительно могут быть указаны следующие сведения: необходимость изготовления экспортируемого ключа электронной подписи, то есть имеющего возможность переноса (копирования) на другой ключевой носитель; ограничения использования ключа электронной подписи и квалифицированного сертификата.

Приложение № 2
к Регламенту (п. 13)

Форма

Начальнику 8 Управления
Генерального штаба Вооруженных Сил
Российской Федерации

ЗАЯВКА
на создание ключей электронных подписей и сертификатов ключей проверки электронных подписей юридического лица

Прошу Ваших указаний о формировании ключей электронных подписей и изготовлении сертификатов ключей проверки электронных подписей:

№ п/п	Фамилия, имя, отчество	Серия и номер паспорта	Наименование организации	Юридический адрес (в соответствии с выпиской из ЕГРЮЛ)	Основной государственный регистрационный номер (ОГРН)	Идентификационный номер налогоплательщика (ИНН)	Страховой номер индивидуального лицевого счета (СНИЛС)	Предназначение электронной подписи	Адрес электронной почты, E-mail
1	2	3	4	5	6	7	8	9	10

Начальник (руководитель) _____
(наименование организации)

_____
(воинское звание, подпись, инициал имени, фамилия)

М.П.

«___» _____ 20__ г.

Примечания: 1. Подпись начальника (руководителя) заверяется печатью установленного образца.

2. В заявке дополнительно могут быть указаны следующие сведения: необходимость изготовления экспортируемого ключа электронной подписи, то есть имеющего возможность переноса (копирования) на другой ключевой носитель; ограничения использования ключа электронной подписи и квалифицированного сертификата.

Приложение № 3
к Регламенту (п. 13)

Форма

Начальнику 8 Управления
Генерального штаба Вооруженных Сил
Российской Федерации

ЗАЯВКА
на создание ключей электронных подписей и сертификатов ключей проверки электронных подписей юридического лица для автоматического создания электронных подписей

Прошу Ваших указаний о формировании ключей электронных подписей и изготовлении сертификатов ключей проверки электронных подписей:

№ п/п	Сокращенное наименование организации (в соответствии с выпиской из ЕГРЮЛ)	Наименование организации	Юридический адрес (в соответствии с выпиской из ЕГРЮЛ)	Основной государственный регистрационный номер (ОГРН)	Идентификационный номер налогоплательщика (ИНН)	Предназначение электронной подписи	Адрес электронной почты, E-mail
1	2	3	4	5	6	7	8

Начальник (руководитель) _____
(наименование организации)

_____
(воинское звание, подпись, инициал имени, фамилия)

М.П.

«___» _____ 20__ г.

Примечания: 1. Подпись начальника (руководителя) заверяется печатью установленного образца.

2. В заявке дополнительно могут быть указаны следующие сведения: необходимость изготовления экспортируемого ключа электронной подписи, то есть имеющего возможность переноса (копирования) на другой ключевой носитель; ограничения использования ключа электронной подписи и квалифицированного сертификата.

Приложение № 4
к Регламенту (п. 31)

Форма

Начальнику 8 Управления
Генерального штаба Вооруженных Сил
Российской Федерации

ЗАЯВКА
на аннулирование (прекращение действия)
сертификатов ключей проверки электронных подписей

Прошу Ваших указаний об аннулировании (прекращении действия) следующих сертификатов ключей проверки электронных подписей:

№ п/п	Серийный номер сертификата ключа проверки электронной подписи	Общее имя*	Основание аннулирования (прекращения действия) сертификата ключа проверки электронной подписи	Дата начала аннулирования (прекращения действия) сертификата ключа проверки электронной подписи
1	2	3	4	5

Начальник (руководитель) _____
(наименование организации)

_____
(воинское звание, подпись, инициал имени, фамилия)

М.П.
«___» _____ 20__ г.

* Имя, фамилия и отчество – для должностного лица или наименование – для юридического лица, указанные в поле «CommonName» («CN») сертификата ключа проверки электронной подписи.

Приложение № 5
к Регламенту (п. 35)

Форма

Начальнику 8 Управления
Генерального штаба Вооруженных Сил
Российской Федерации

ЗАЯВКА
на изменение статуса сертификатов ключей проверки электронных подписей

Прошу Ваших указаний о приостановлении/возобновлении действия следующих сертификатов ключей проверки электронных подписей:

№ п/п	Серийный номер сертификата ключа проверки электронной подписи	Общее имя*	Основание изменения статуса сертификата ключа проверки электронной подписи	Дата начала изменения статуса сертификата ключа проверки электронной подписи
1	2	3	4	5

Начальник (руководитель) _____
(наименование организации)

_____
(воинское звание, подпись, инициал имени, фамилия)

М.П.
«___» _____ 20__ г.

* Имя, фамилия и отчество – для должностного лица или наименование – для юридического лица, указанные в поле «CommonName» («CN») сертификата ключа проверки электронной подписи.

Приложение № 6
к Регламенту (п. 46)

Форма

Начальнику 8 Управления
Генерального штаба Вооруженных Сил
Российской Федерации

ЗАЯВКА
на получение информации о статусе сертификатов ключей проверки электронных подписей

Прошу Ваших указаний о предоставлении информации о статусе сертификатов ключей проверки электронных подписей:

№ п/п	Серийный номер сертификата ключа проверки электронной подписи	Общее имя*	Время и дата, на момент наступления которых требуется установить статус сертификата ключа проверки электронной подписи** (с _ _ ч _ _ мин ___ ___ 20___ г. по ___ ч ___ мин ___ ___ 20___ г.)
1	2	3	4

Начальник (руководитель) _____
(наименование организации)

_____
(воинское звание, подпись, инициал имени, фамилия)

М.П.
«___» _____ 20__ г.

* Имя, фамилия и отчество – для должностного лица или наименование – для юридического лица, указанные в поле «CommonName» («CN») сертификата ключа проверки электронной подписи.

** Время и дата должны быть указаны с учетом часового пояса г. Москвы (по московскому времени). Если время и дата не указаны, то статус сертификата ключа проверки электронной подписи устанавливается на дату подписи заявки.