Приложение № 2
к Правилам электронного документооборота
ООО КБ “Интеграл”

ОРГАНИЗАЦИЯ УПРАВЛЕНИЯ КЛЮЧЕВЫМИ СИСТЕМАМИ В СЭД.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Организатор СЭД обеспечивает функционирование СЭД с использованием СКЗИ «Бикрипт-КСБ-М» СКЗИ «Криптоком 3.1», каждая из которых эксплуатируется с собственной ключевой системой.

1.2. Структурное подразделение Организатора СЭД, обеспечивающее управление ключевыми системами в СЭД – группа технических средств и телекоммуникаций отдела автоматизации. Данное подразделение выполняет функции Центра Управления Ключевыми Системами (ЦУКС). Указанное структурное подразделение обеспечивает выработку закрытых (секретных) ключей шифрования и закрытых (секретных) ключей электронной подписи для Организатора СЭД, а в случае необходимости – и для Участников СЭД; осуществляет регистрацию открытых (публичных) ключей шифрования и открытых (публичных) ключей электронной подписи Организатора СЭД и Участников СЭД в соответствующих справочниках открытых (публичных) ключей, взаимодействует с Участниками СЭД при их регистрации, проведении плановой замены криптографических ключей, замены криптографических ключей в случае их компрометации. Внесение изменений в справочники открытых (публичных) ключей выполняется Организатором СЭД по рабочим дням с 9.00 до 18.00 по московскому времени. В случае необходимости по усмотрению Организатора СЭД изменения в справочники открытых (публичных) ключей могут быть внесены и в другое время..

1.3. Участники СЭД признают, что используемые в СЭД СКЗИ обеспечивают достаточную конфиденциальность электронного документооборота и позволяют идентифицировать владельца открытого (публичного) ключа электронной подписи, а также установить отсутствие искажения информации в электронном документе.

1.4. Закрытые (секретные) ключи электронной подписи и шифрования Участника СЭД и соответствующие им открытые (публичные) ключи электронной подписи, регистрируемые Организатором СЭД, имеют ограниченный срок действия. Периодичность плановой смены закрытых (секретных) ключей шифрования и электронной подписи устанавливается равной 1 году. Дата проведения плановой смены ключей определяется организатором СЭД.

1.5. Участник СЭД не может подписать электронный документ своей электронной подписью или произвести зашифрование/расшифрование информации в текущий момент времени, если к этому времени истек срок действия его закрытых (секретных) ключей электронной подписи или шифрования. Также Участник СЭД не может проверить электронную подпись электронного документа или произвести расшифрование информации в случае вывода из действия открытого (публичного) ключа электронной подписи, необходимого для выполнения соответствующей операции.

1.6. Участник СЭД не должен хранить электронные документы в архивах в зашифрованном виде. Шифрование ЭД осуществляется только для обеспечения конфиденциальности информации при транспортировке ЭД от Участника СЭД к Организатору СЭД и в обратном направлении.

1.7. Участник СЭД не обязан получать какую-либо дополнительную лицензию на право эксплуатации используемых в СЭД СКЗИ. При этом Участник СЭД обязан использовать предоставленные Организатором СЭД СКЗИ только для работы в СЭД, а также обеспечивать возможность контроля использования СКЗИ со стороны Организатора СЭД.

1.8. Услуги Организатора СЭД по изготовлению криптографических ключей и регистрации открытых (публичных) ключей электронной подписи и/или шифрования, предоставлению СКЗИ и иных программно-технических средств, а также услуги, связанные с организацией электронного документооборота в соответствии с Правилами электронного документооборота, являются платными. Порядок оплаты и расценки (тарифы) на эти услуги утверждаются Правлением Организатора СЭД. Информация о порядке оплаты и расценках опубликовывается на WEB-сервере Организатора СЭД.

1.9. В процессе эксплуатации СКЗИ Участник СЭД обязуется соблюдать лицензионные ограничения разработчиков СКЗИ, а также выполнять рекомендации по обеспечению безопасности информации при эксплуатации СКЗИ (раздел 7 настоящего Приложения).

1.10. Владельцем открытого (публичного) ключа электронной подписи в СЭД является физическое лицо – полномочный представитель Участника СЭД. Полномочия данного лица подтверждаются учредительными документами Участника СЭД или выданной данному лицу доверенностью, подписанной руководителем организации Участника СЭД и заверенной печатью Участника СЭД.

1.11. Организатор СЭД обеспечивает хранение открытых (публичных) ключей электронной подписи и шифрования Участников СЭД в электронном виде и документов на бумажном носителе – регистрационных карточек открытых (публичных) ключей электронной подписи и/или шифрования, а также возможность получения открытых (публичных) ключей электронной подписи Участников СЭД в электронном виде в течение всего установленного срока хранения документов, подписанных соответствующими закрытыми (секретными) ключами.

2. ПОРЯДОК ФОРМИРОВАНИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ УЧАСТНИКА СЭД

2.1. Участник СЭД предоставляет Организатору СЭД пакет документов, необходимых для формирования криптографических ключей Участника СЭД.

2.2. Пакет документов включает Заявление Участника СЭД на изготовление ключей шифрования и регистрацию открытых (публичных) ключей электронной подписи, подписанное полномочным представителем Участника СЭД, руководителем и главным бухгалтером (при его наличии в штате) организации Участника СЭД и заверенное печатью Участника СЭД (раздел 8 настоящего Приложения), и доверенность на полномочного представителя Участника СЭД, на чье имя будет регистрироваться открытый (публичный) ключ электронной подписи Участника СЭД (раздел 9 настоящего Приложения) – за исключением случая регистрации открытого (публичного) на имя руководителя организации Участника СЭД.

2.3. Организатор СЭД осуществляет проверку правильности указанных Участником СЭД данных в переданных документах.

2.4. Участник СЭД оплачивает услуги Организатора СЭД по изготовлению ключей шифрования и регистрации открытых (публичных) ключей электронной подписи и предоставлению СКЗИ (при получении новых СКЗИ). В случае генерации закрытых (секретных) ключей электронной подписи Участника СЭД Организатором СЭД, Участник СЭД оплачивает эту услугу дополнительно.

2.5. Полномочный представитель Участника СЭД при первичном изготовлении сертификата ключа электронной подписи должен пройти процедуру регистрации у Организатора СЭД.

2.6. Сформированные ключи шифрования и СКЗИ, техническая документация передаются Участнику СЭД через полномочного представителя на основании доверенности (раздел 10 настоящего Приложения).

2.7. После получения СКЗИ и ключей шифрования полномочный представитель Участника СЭД должен на клиентском рабочем месте изготовить личные закрытые (секретные) ключи электронной подписи и соответствующие им открытые (публичные) ключи электронной подписи, а также изготовить 2 экземпляра регистрационной карточки открытых (публичных) ключей (Разделы 13 и 14 настоящего приложения). Участник СЭД устанавливает порядок хранения и использования ключевых носителей с закрытыми (секретными) ключами своих полномочных представителей, а также количество и порядок хранения резервных копий этих ключевых носителей в соответствии с рекомендациями раздела 7 настоящего Приложения.

2.8. Регистрационные карточки открытых (публичных) ключей электронной подписи вместе в файлом, содержащим открытый ключ полномочного представителя Участника СЭД передается Участником СЭД Администратору безопасности Организатора СЭД любым доступным способом.

2.9. Администратор безопасности Организатора СЭД после получения файла открытого (публичного) ключа электронной подписи и соответствующих ему регистрационных карточек в течение 2-х рабочих дней регистрирует открытый (публичный) ключ электронной подписи полномочного представителя Участника СЭД в справочнике открытых ключей Организатора СЭД и заверяет регистрационную карточку открытого (публичного) ключа полномочного представителя Участника СЭД собственноручной подписью и печатью Центра управления ключевыми системами Организатора СЭД.

2.10. Участник СЭД получает от Организатора СЭД вместе с заверенной Организатором СЭД регистрационной карточкой открытого ключа полномочного представителя Участика СЭД карточку отзыва открытого (публичного) ключа электронной подписи.

2.11. Инсталляция СКЗИ и иных программных средств на клиентском рабочем месте производится Участником СЭД самостоятельно в соответствии с передаваемой ему документацией.

2.12. Изготовленные закрытые (секретные) ключи передаются Участнику СЭД через полномочного представителя на основании доверенности (раздел 10 настоящего Приложения).

2.13. Открытые (публичные) ключи электронной подписи Организатора СЭД в форме документов на бумажном носителе при необходимости предоставляются Участникам СЭД в виде копий, заверенных Организатором СЭД.

3. ПОРЯДОК ДЕЙСТВИЙ УЧАСТНИКА СЭД ПРИ ПРОВЕДЕНИИ ПЛАНОВОЙ ЗАМЕНЫ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

3.1. Срок действия закрытых (секретных) ключей электронной подписи и шифрования при формировании сертификата ключа электронной подписи полномочного представителя Участника СЭД устанавливается равным 1-му году. Дата плановой смены ключей определяется Организатором СЭД и доводится до Участников СЭД электронным документом категории «А» не позднее чем за 1 месяц до ее наступления.

3.2. В течение периода с момента объявления даты плановой смены ключей до ее наступления Участник СЭД обязан получить у Организатора СЭД новые закрытые (секретные) ключи шифрования и произвести формирование новых закрытых (секретных) и открытых (публичных) ключей электронной подписи, оформить Регистрационные карточки открытых (публичных ключей) электронной подписи и новую доверенность на своего полномочного представителя и передать их Организатору СЭД Порядок действий Участника СЭД при регистрации нового открытого (публичного) ключа электронной подписи представлен в разделе 2 настоящего Приложения.

3.3. Участник СЭД получает сформированный Организатором СЭД новый справочник открытых (публичных) ключей электронной подписи у Организатора СЭД при прохождении процедуры регистрации новых открытых (публичных) ключей электронной подписи и устанавливает его на клиентском рабочем месте при наступлении даты плановой смены ключей.

3.4. Ключевые носители с закрытыми (секретными) ключами электронной подписи и шифрования, срок действия которых истек, должны уничтожаться путем двойного переформатирования.

3.5. Срок хранения справочников открытых (публичных) ключей электронной подписи у Участника СЭД определен правилами электронного документооборота и должен составлять не менее 3 лет с момента истечения срока их действия.

4. ПОРЯДОК ДЕЙСТВИЙ ПРИ КОМПРОМЕТАЦИИ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ УЧАСТНИКА СЭД

4.1. К событиям, на основании которых лицо, владеющее закрытым (секретным) ключом электронной подписи и/или шифрования, принимает решение о его компрометации, относятся, включая, но, не ограничиваясь, следующие:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевым носителям;
- возникновение подозрений на утечку информации или ее искажение в СЭД;
- нарушение правил хранения ключевых носителей.

4.2. В случае принятия решения о компрометации своих криптографических ключей Участник СЭД обязан по телефону сообщить Администратору безопасности Организатора СЭД о факте компрометации используемых закрытых (секретных) ключей с использованием пароля, указанного в карточке отзыва открытого (публичного) ключа, получить и прекратить использование скомпрометированных криптографических ключей для информационного обмена с Организатором СЭД.

4.3. В течение одного рабочего дня Участник СЭД обязан направить Администратору безопасности Организатора СЭД письменное уведомление, подписанное руководителем организации и заверенное печатью Участника СЭД, о факте компрометации закрытых (секретных) ключей. Форма уведомления приведена в разделе 11 настоящего приложения.

4.4. При представлении уведомления о компрометации закрытых (секретных) ключей электронной подписи полномочный представитель Участника СЭД обязан получить у Организатора СЭД новые закрытые (секретные) ключи шифрования и произвести формирование новых закрытых (секретных) и открытых (публичных) ключей электронной подписи, оформить Регистрационные карточки открытых (публичных ключей) электронной подписи и новую доверенность на своего полномочного представителя и передать их Организатору СЭД Порядок действий Участника СЭД при регистрации нового открытого (публичного) ключа электронной подписи представлен в разделе 2 настоящего Приложения

4.5. При получении голосового сообщения о компрометации Администратор безопасности Организатора СЭД блокирует использование соответствующего скомпрометированному закрытому (секретному) ключу открытого (публичного) ключа в СЭД. Дата и время, с которого открытый (публичный) ключ электронной подписи считается недействительным в СЭД, устанавливается равным времени получения письменного уведомления о компрометации, подписанного уполномоченным должностным лицом Участника СЭД.

4.6. Открытый (публичный) ключ электронной подписи, соответствующий скомпрометированным закрытым (секретным) ключам, исключается из ключевой базы Организатора СЭД и хранится в течение срока хранения документов, подписанных скомпрометированным закрытым (секретным) ключа электронной подписи для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением электронной подписи.

5. АННУЛИРОВАНИЕ ОТКРЫТОГО (ПУБЛИЧНОГО) КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ УЧАСТНИКА СЭД

5.1. Организатор СЭД аннулирует открытый (публичный) ключ электронной подписи Участника СЭД в следующих случаях:

- после осуществления плановой смены криптографических ключей;
- в случае прекращения действия Договора о присоединении Участника СЭД к СЭД в отношении данного Участника СЭД;
- по заявлению в письменной форме Участника СЭД, подписанного руководителем организации Участника СЭД и заверенного печатью Участника СЭД.

5.2. В случае аннулирования открытого (публичного) ключа электронной подписи Участника СЭД Организатор СЭД исключает его справочника открытых (публичных) ключей электронной подписи Открытый (публичный) ключ хранится в течение срока хранения документов, подписанных аннулируемым закрытым (секретным) ключом электронной подписи для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением электронной подписи.

5.3. Дата и время, с которого открытый (публичный) ключ электронной подписи считается недействительным в СЭД, устанавливается равным времени наступления обстоятельств, перечисленных в п. 5.1.

6. ПОРЯДОК ПРОВЕДЕНИЯ ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ ПРИ РАЗРЕШЕНИИ КОНФЛИКТНЫХ СИТУАЦИЙ

6.1. В случае возникновения конфликтной ситуации при применении электронной подписи, такая ситуация подлежит разрешению в порядке, установленном Правилами электронного документооборота с учетом особенностей, установленных настоящим Приложением.

6.2. Проведение технической экспертизы при разрешении подобных конфликтных ситуаций в соответствии с особенностями технологии электронной подписи требует применения специального программного обеспечения для выполнения необходимых проверок и документирования данных, используемых при выполнении необходимых проверок.

6.3. Протокол проверки электронной подписи, формируемый специальным программным обеспечением, является основным документом работы технической комиссии и должен быть подписан всеми членами комиссии.

6.4. Для проведения технической экспертизы необходимы:

- файл электронного документа, в отношении которого возникла конфликтная ситуация;
- программное обеспечение для работы с контрольными архивами электронных документов (разбора конфликтных ситуаций);
- ключевая база Центра управления ключевыми системами Организатора СЭД, содержащая открытые (публичные) ключи электронной подписи, отобранные для разбора конфликтной ситуации.
- Карточки регистрации открытых (публичных) ключей электронной подписи, уведомления о компрометации, заявления об аннулировании открытых (публичных) , отобранные для разбора конфликтной ситуации

6.5. Проведение технической экспертизы для конкретного электронного документа включает в себя выполнение следующих действий:

- определение открытого (публичного) ключа электронной подписи или нескольких открытых (публичных) ключей электронной подписи, необходимых для проверки электронной подписи;

- проверку электронной подписи электронного документа с использованием каждого открытого (публичного) ключа электронной подписи из отобранных для разбора конфликтной ситуации;
- определение даты формирования каждой проверяемой электронной подписи в электронном документе;
- проверку правильности и времени оформления регистрационной карточки открытого (публичного) ключа электронной подписи Организатором СЭД для каждого открытого (публичного) ключа электронной подписи, отобранного для разбора конфликтной ситуации;
- проверку действительности открытых (публичных) ключей электронной подписи, отобранных для разбора конфликтной ситуации, на момент формирования электронной подписи;
- проверку отсутствия принятых в установленном порядке Организатором СЭД уведомлений о компрометации закрытого (секретного) ключа электронной подписи или заявления об аннулировании открытого (публичного) ключа электронной подписи на момент получения документа Организатором СЭД.

6.6. В случае, если:

- все проверяемые электронные подписи для данного ЭД верны;
- содержание регистрационной карточки открытого (публичного) ключа соответствует открытому (публичному) ключу, находящемуся в справочнике открытых (публичных) ключей Организатора СЭД;
- отсутствуют или представлены позднее времени приема документа Организатором СЭД принятые в установленном порядке Организатором СЭД уведомления о компрометации закрытого (секретного) ключа электронной подписи или заявление об аннулировании открытого (публичного) ключа электронной подписи ;

считается установленным:

- что проверяемый ЭД был сформирован в соответствии с Правилами электронного документооборота и требованиями законодательства Российской Федерации;
- проверяемый ЭД был подписан на закрытых (секретных) ключах электронной подписи, соответствующих открытым (публичным) ключам электронной подписи, использовавшимся при проведении технической экспертизы;
- владельцами открытых (публичных) ключей электронной подписи являются полномочные представители Участников СЭД, зарегистрированные Организатором СЭД.

7. РЕКОМЕНДАЦИИ УЧАСТНИКУ СЭД ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ СКЗИ

7.1. Режим эксплуатации СКЗИ, применяемых в СЭД, устанавливается в соответствии с "Требованиями к средствам криптографической защиты конфиденциальной информации" по уровню "КС1".

7.1.1. Рекомендации по организационному обеспечению безопасности СКЗИ:

- в организации Участника СЭД выделяются (определяются) должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СКЗИ;
- в организации Участника СЭД разрабатываются нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ;
- к работе с СКЗИ допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации СКЗИ.

7.1.2. Рекомендации по размещению СКЗИ и режиму охраны:

- помещения, в которых размещаются технические средства клиентского рабочего места со встроенными СКЗИ, являются режимными и должны обеспечивать конфиденциальность проводимых работ;
- размещение режимных помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств;
- размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности;
- входные двери режимных помещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время;
- окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией;
- размещение технических средств в режимном помещении должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается, через окна;
- в режимные помещения допускаются руководители организации Участника СЭД, сотрудники подразделения безопасности и исполнители, имеющие прямое отношение к обработке, передаче и приему конфиденциальных документов;
- системные блоки компьютеров с СКЗИ оборудуются средствами контроля вскрытия;
- ремонт и/или последующее использование системных блоков осуществляется после удаления с них программного обеспечения СКЗИ.

7.1.3. Рекомендации по обеспечению безопасности ключевой информации:

- ключевые носители с закрытыми (секретными) ключами электронной подписи и шифрования и инсталляционные дискеты с программным обеспечением СКЗИ в организации Участника СЭД берутся на поэкземплярный учет в выделенных для этих целей журналах;
- учет и хранение закрытых (секретных) ключей поручается руководством организации Участника СЭД специально выделенным сотрудникам;
- для хранения ключевых носителей с закрытыми (секретными) ключами электронной подписи и шифрования выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации;
- хранение ключей и инсталляционных дискет с программным обеспечением СКЗИ допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение;
- при транспортировке ключевых носителей с закрытой (секретной) ключевой информацией создаются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.

Примечание: Настоящие рекомендации Участнику СЭД определяются условиями лицензирования деятельности Организатора СЭД при использовании сертифицированных СКЗИ, а также правилами эксплуатации СКЗИ.

8. ФОРМА ЗАЯВЛЕНИЯ УЧАСТНИКА СЭД НА РЕГИСТРАЦИЮ ОТКРЫТОГО (ПУБЛИЧНОГО) КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ

(Оформляется на бланке организации)

Администратору безопасности Организатора СЭД

Заявление
на регистрацию открытого (публичного) ключа электронной подписи

№_____ "___" _____ 200_ г.

В целях использования в СЭД:

1. Просим Вас предоставить СКЗИ для установки на клиентском рабочем месте в организации Участника СЭД.
2. Просим Вас самостоятельно изготовить наши закрытые (секретные) ключи шифрования.
3. Просим Вас самостоятельно изготовить наши закрытые (секретные) ключи электронной подписи.
4. Просим Вас зарегистрировать открытый (публичный) ключ электронной подписи полномочного представителя Участника СЭД

_____
(полное наименование организации Участника СЭД)

со следующими регистрационными данными :

4.1 .Владелец открытого (публичного) ключа электронной подписи (полномочный представитель Участника СЭД):

Должность . . . . . .
Фамилия . . . . . .
Имя . . . . . .
Отчество . . . . . .
E-Mail . . . . . .

Действует на основании: ☐ Учредительных документов (Устава) ☐ Доверенности

5. Оплату перечисленных в Заявлении услуг Организатора СЭД гарантируем.
6. Настоящим Участник СЭД

_____
(полное наименование организации Участника СЭД)

заявляет, что любые действия, которые будут совершены владельцем открытого (публичного) ключа электронной подписи Участника СЭД на основании настоящего открытого (публичного) ключа являются действиями, совершаемыми владельцем открытого (публичного) ключа электронной подписи от имени Участника СЭД, по его указанию и связаны с участием в электронном документообороте в процессе осуществления предпринимательской деятельности Участника СЭД.

6. Контактное лицо Участника СЭД, ответственное за эксплуатацию СКЗИ

_____
(должность, ФИО, телефон, E-Mail)

Полномочный представитель Участника СЭД _____ / Фамилия И.О. /
(владелец открытого (публичного) ключа электронной подписи)
Руководитель организации Участника СЭД _____ / Фамилия И.О. /
Главный бухгалтер организации Участника СЭД _____ / Фамилия И.О. /

М.П.

9. ФОРМА ДОВЕРЕННОСТИ НА ПОЛНОМОЧНОГО ПРЕДСТАВИТЕЛЯ УЧАСТНИКА СЭД ДЛЯ РАБОТЫ С ОТКРЫТЫМ (ПУБЛИЧНЫМ) КЛЮЧЕМ ЭЛЕКТРОННОЙ ПОДПИСИ

(Оформляется на бланке организации)

Доверенность № _____

г. _____ _____
(место выдачи) (дата выдачи)

_____, далее – Участник СЭД,
(полное наименование организации Участника СЭД)

в лице _____, действующего на
(должность, фамилия, имя, отчество)

основании Устава, уполномочивает _____
(должность, фамилия, имя, отчество полномочного представителя)

- *паспортные данные: серия, номер, орган, выдавший паспорт, дата выдачи;*
- *телефон для связи,*

на выполнение следующих действий в соответствии с требованиями Правил электронного документооборота:

- подписывать собственноручной подписью документы, необходимые для регистрации открытых (публичных) ключей электронной подписи:
  1) заявление Участника СЭД на регистрацию открытого (публичного) ключа электронной подписи;
  2) регистрационную карточку открытого (публичного) ключа электронной подписи полномочного представителя Участника СЭД, владельцем которого является указанное доверенное лицо;
- использовать соответствующие криптографические ключи в течение сроков их действия от имени Участника СЭД, по его указанию и в связи с участием в электронном документообороте в процессе осуществления предпринимательской деятельности Участника СЭД.

Настоящая доверенность действительна до "_____" _____ 200__ года.

Подпись (фамилия, инициалы) _____ удостоверем.
(личная подпись)

Руководитель _____ _____ (инициалы, фамилия)
(наименование должности) (личная подпись)

Главный бухгалтер _____ (инициалы, фамилия)
(личная подпись)

М.П.

10. ФОРМА ДОВЕРЕННОСТИ НА ПОЛУЧЕНИЕ ДОКУМЕНТОВ, ПРОГРАММНОГО И ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДЛЯ РАБОТЫ С СЕРТИФИКАТАМИ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ

(Оформляется на бланке организации)

Доверенность № _____

г. _____ _____
(место выдачи) (дата выдачи)

_____, далее – Участник СЭД,
(полное наименование организации Участника СЭД)

в лице _____, действующего на
(должность, фамилия, имя, отчество)

основании Устава, уполномочивает _____
(должность, фамилия, имя, отчество полномочного представителя)

- *паспортные данные: серия, номер, орган, выдавший паспорт, дата выдачи;*
- *телефон для связи,*

на выполнение следующих действий:

- получать программное обеспечение со встроенными СКЗИ для установки и работы на клиентском рабочем месте Участника СЭД;
- получать закрытые (секретные) ключи электронной подписи и/или шифрования Участника СЭД
- получать карточку оповещения о компрометации закрытых (секретных) ключей электронной подписи и/или шифрования (Раздел 12 настоящего приложения);
- получать идентификаторы и пароли Участника СЭД, необходимые для работы в СЭД.

Настоящая доверенность действительна до "_____" _____ 200__ года.

Подпись (фамилия, инициалы) _____ удостоверяю.
(личная подпись)

Руководитель _____ _____ (инициалы, фамилия)
(наименование должности) (личная подпись)

Главный бухгалтер _____ (инициалы, фамилия)
(личная подпись)

М.П.

Примечание:
Участник СЭД может предоставить своему представителю другие полномочия, необходимые для выполнения действий в соответствии с Правилами электронного документооборота.

11. ФОРМА УВЕДОМЛЕНИЯ О КОМПРОМЕТАЦИИ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

(Оформляется на бланке организации)

Администратору безопасности Организатора СЭД

Уведомление о компрометации криптографических ключей

№_____ " ___" _____ 200_ г.

Настоящим уведомляю о компрометации криптографических ключей, идентифицируемых перечисленными ниже параметрами:

Идентификатор открытого ключа электронной подписи _____
использовавшихся в

_____
(полное наименование организации Участника СЭД)

владельцем открытого ключа электронной подписи

_____
(фамилия, имя, отчество полномочного представителя Участника СЭД)

в соответствии с Правилами электронного документооборота.
Данные криптографические ключи прошу считать скомпрометированными и выведенными из действия с "_____" _____ 200__ г. ___ часов ____ минут

Руководитель организации _____ / Фамилия И.О. /

М.П.

Примечание:

1. Время вывода криптографических ключей из действия, указываемая в настоящем Уведомлении, не может быть ранее даты получения данного Уведомления Организатором СЭД или получения сообщения о компрометации Администратором безопасности Организатора СЭД.
2. В случае если Участник СЭД, формирующий настоящее Уведомление, ранее сообщил Администратору безопасности Организатора СЭД о компрометации данных криптографических ключей по телефону, то в настоящем Уведомлении время вывода криптографических ключей из действия определяется временем соответствующего сообщения по телефону.

12 ФОРМА ЗАЯВЛЕНИЯ ОБ АННУЛИРОВАНИИИ ОТКРЫТОГО (ПУБЛИЧНОГО) КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ УЧАСТНИКА СЭД

(Оформляется на бланке организации)

Администратору безопасности Организатора СЭД

Заявление об аннулировании открытого (публичного) ключа электронной подписи

№_____ " ___" _____ 200_ г.

Прошу Вас аннулировать открытый (публичный) ключ электронной подписи, идентифицируемый перечисленными ниже параметрами:

Идентификатор открытого ключа электронной подписи _____

использовавшийся в

_____
(полное наименование организации Участника СЭД)

владельцем открытого (публичного) ключа электронной подписи

_____
(фамилия, имя, отчество полномочного представителя Участника СЭД)

в соответствии с Правилами электронного документооборота.
Данный открытый (публичный) ключ прошу считать аннулированным и выведенным из действия с "_____" _____ 200__ г.

Руководитель организации _____ / Фамилия И.О. /

М.П.

13. ФОРМА КАРТОЧКИ УВЕДОМЛЕНИЯ О КОМПРОМЕТАЦИИ ЗАКРЫТЫХ (СЕКРЕТНЫХ) КЛЮЧЕЙ ШИФРОВАНИЯ И/ИЛИ ЭЛЕКТРОННОЙ ПОДПИСИ УЧАСТНИКА СЭД

Карточка оповещения о компрометации
закрытых (секретных) ключей шифрования и/или электронной подписи
Участника СЭД _____
(полное наименование организации Участника СЭД)

	Телефон	Пароль
Администратор безопасности Организатора СЭД	795-0760 доб. 109	<пароль администратора безопасности>
Контактное лицо Участника СЭД, ответственное за эксплуатацию СКЗИ	<телефон>	<пароль участника СЭД>

Администратор безопасности
Организатора СЭД _____ /Фамилия И.О./
М.П.

14. ФОРМА РЕГИСТРАЦИОННОЙ КАРТОЧКИ ОТКРЫТОГО (ПУБЛИЧНОГО) КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ ПОЛНОМОЧНОГО ПРЕДСТАВИТЕЛЯ УЧАСТНИКА СЭД (ДЛЯ СКЗИ БИКРИПТ-КСМ-Б)

Регистрационная карточка
открытого (публичного) ключа электронной подписи Участника СЭД

Участник СЭД ____
(полное наименование организации Участника СЭД)

Владелец открытого (публичного) ключа электронной подписи (полномочный представитель Участника СЭД):

Должность . . . .
Фамилия . . . .
Имя . . . .
Отчество . . . .
E-Mail . . . .

Идентификатор открытого (публичного) ключа электронной подписи _____________

Открытый (публичный) ключ электронной подписи:

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Полномочный представитель
Участника СЭД ________________________________/Фамилия И.О/
Руководитель организации
Участника СЭД ________________________________/Фамилия И.О/
Главный бухгалтер
Участника СЭД ________________________________/Фамилия И.О/
М.П.

Полномочия должностных лиц Участника СЭД проверены, их подписи с карточкой образцов подписей сверены:

Начальник ОПЕРО
Организатора СЭД ________________________________/Фамилия И.О/
М.П.
Открытый ключ зарегистрирован “__” ___________ 200__ года в ___ часов ___ минут.

Администратор безопасности
Организатора СЭД ________________________________/Фамилия И.О/
М.П.

15. ФОРМА ЗАПРОСА НА РЕГИСТРАЦИЮ ОТКРЫТОГО (ПУБЛИЧНОГО) КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ ПОЛНОМОЧНОГО ПРЕДСТАВИТЕЛЯ УЧАСТНИКА СЭД (ДЛЯ СКЗИ КРИПТОКОМ 3.1)

ЗАПРОС НА РЕГИСТРАЦИЮ ОТКРЫТОГО (ПУБЛИЧНОГО) КЛЮЧА И ВЫПУСК СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ ПОЛНОМОЧНОГО ПРЕДСТАВИТЕЛЯ УЧАСТНИКА СЭД

Участник СЭД: <Наименование Участника СЭД>
Владелец открытого (публичного) ключа -
Полномочный представитель участника СЭД: <Фамилия, Имя, Отчество полномочного представителя Участника СЭД>
Должность: <должность полномочного представителя Участника СЭД>
Страна: <страна регистрации Участника СЭД>
Регион: <регион регистрации Участника СЭД>
Населенный пункт: <населенный пункт регистрации Участника СЭД
Адрес электронной почты: <адрес электронной почты полномочного представителя Участника СЭД>
Открытый (публичный) ключ полномочного представителя Участника СЭД:

```
            Public Key Algorithm: r3410
            R3410 Public Key:
                pub:  (1023 bits)
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00
                P:    (1024 bits)
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00
                Q:    (256 bits)
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00
                A:    (1024 bits)
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
                    00:00:00:00:00:00:00:00
        Attributes:
            00:00
    Signature Algorithm: r3410WithR3411
        00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
        00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
        00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
        00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
```

Запрос на сертификат (в формате PEM):

```
-----BEGIN CERTIFICATE REQUEST-----
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
```

```
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000
-----END CERTIFICATE REQUEST-----
```

Полномочный представитель
Участника СЭД _____/Фамилия И.О/
Руководитель организации
Участника СЭД _____/Фамилия И.О/
Главный бухгалтер
Участника СЭД _____/Фамилия И.О/
М.П.

Полномочия должностных лиц Участника СЭД проверены, их подписи с карточкой образцов подписей сверены:

Начальник ОПЕРО
Организатора СЭД _____/Фамилия И.О/
М.П.
Открытый ключ зарегистрирован “__” _____ 200__ года в ___ часов ___ минут.

Администратор безопасности
Организатора СЭД _____/Фамилия И.О/
М.П.